Technical Report 2008N5-SP-NL
Networking Lab, KHU, South Korea

Security Attacks and Challenges in Wireless Sensor Networks

Chapter 1

Introduction

Wireless Sensor Networks (WSNs) [1] offer a unique way of extracting data from hazardous geographical regions where human intervention is extremely difficult, the network is often unattended, and where a specified level of security has to be maintained for each step of the network's operation. Among all varieties of wireless networks, WSNs are the type of networks that demand high-level security as one of their core features. In practical terms, a WSN is considered a class of ad hoc networks which can form whenever needed, sometimes without a fixed infra-structure. We define a sensor network as a network consisting of a set of small sensor devices that are deployed in an ad hoc fashion to cooperate with each other for sensing certain physical phenomenon. Typically a WSN has one or more base stations (sometimes called as sink) and a large number of sensing devices.

Various issues in WSNs are still under investigation and many of them have yet to reach desired standards. Over the past few decades, with the advancements of ad hoc networking technologies, the research on WSNs has also been benefited. However, because of the differences in the nature of the works and the constrained resources of WSNs, many solutions that are devised for traditional ad hoc networks will not work for WSNs.

Security in wireless sensor network has a great number of challenges, ranging from the nature of wireless communications, constrained resources of the sensors, unknown topologies of the deployed networks, unattended environment where sensors might be susceptible to physical attacks, dense and large networks, etc. [2], [3]. In fact, each of these issues leads to different research direction. Whenever we think about any feasible security scheme for WSNs, we focus on a specific aspect and often ignore the other associated threats. It is in reality impossible to deal with all the security threats with a single mechanism. Hence, the approach is often to choose the most appropriate mechanism, based on the situation at hand and the settings of the network.

From the high-level point of view, we consider the following six principles while considering security for any system. These are collectively known as the philosophy of mistrust:

- Don’t talk to any one you don’t know
- Accept nothing without a guarantee
- Take everyone as an enemy until proved otherwise
- Don’t trust your friend for long
- Use well-tried solutions
- Watch the ground you are standing on for cracks

Maintaining all these principles at the same time requires a lot of

computational, memory, and energy resources which are not available in wireless sensor networks. Many security solutions that are well-established for other wireless networks are often not fit for direct use in WSNs and any security solution that needs periodic renewal of any security component (e.g., secret key, secret hash value, session key, etc.) might not at all be viable because of the energy constraints. Considering these factors, devising efficient security mechanisms for WSNs is a challenging issue.

1.1 Background

Wireless sensor network is a special class of wireless ad hoc networks. Hence, we think that a comparative discussion about security issues in wireless ad hoc networks and sensor networks could be beneficial for the readers. However, detailed discussion on the security issues of ad hoc networks is out of the scope of this report. Also for brevity of the comparative discussion and the reference section of this report, we have opted not to put extra references regarding the security related works in wireless ad hoc networks.

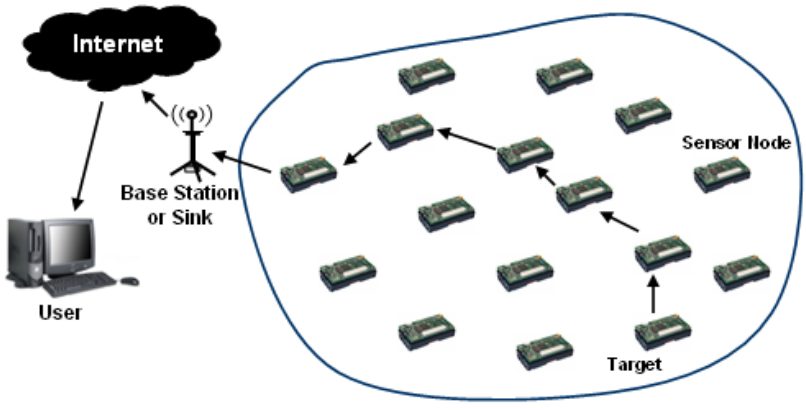

Figure 1-1. A typical wireless sensor network

The major difference in security considerations for wireless ad hoc networks and that are in wireless sensor network lies in the inherent structural and

characteristic differences of these two networks. We know that WSN is a type of ad hoc network that has some type of infrastructure. There is a central entity that is called sink or base station which is responsible for collecting data from the sensors deployed in the field. The sensors in the field could be dispersed randomly, however there is a hierarchy of entities that could be used for dealing with various security aspects in WSN. So, for any security mechanism, in case of WSN we have a powerful entity who could serve the managerial tasks. On the other hand, in case of ad hoc networks or especially for mobile ad hoc networks (MANETs), each node acts as a routing entity as well as a host. Hence, without the central entity or a supporting infrastructure, the security mechanisms must be designed and developed. So far, there have many works in MANET security. All the works could be categorized mainly into: link layer security schemes, cooperative security schemes, and secure packet forwarding schemes. As each node is independent, cooperative schemes are often effective where each node is responsible for maintaining its own security and a group of nodes cooperate with each other for dealing any security threat and attack. Secure forwarding of packets is basically a part of secure routing. There have been many secure routing protocols for MANETs like ARAN [136], ARIADNE [137], S-AODV [138], etc.; however because of the nature of works and organization of the network, secure routing in WSN differs from those solutions. In most of the cases, it is not possible to directly utilize the secure routing techniques for WSNs. Besides the structural differences, the reason for this is the considered amount of resources in case of MANETs which are not the case for WSNs. As we mentioned earlier, we have opted not to put all the references for brevity of this report. Also after some studies, we have found that it would be beneficial to explore the special cases present in WSN in case of security.

Before an in-depth investigation of the security threats and attacks in wireless sensor networks (a typical model of wireless sensor network is shown in Figure

1-1), let us first look at the major aspects that make the issue of maintaining security difficult for wireless sensor networks.

1.1.1 Key Aspects to Consider for WSN Security

Constrained Resources of Sensors - The sensors that build up the network are usually of inadequate memory, processing, and communication capabilities and cannot support the execution of a large amount of code. Their energy sources are also very limited. As an example, Crossbow MICA2 mote (shown in Figure 1-2) [4] is a well-known sensor node with an ATmega128L 8-bit processor at 8 MHz, 128KB program memory (flash), 512KB additional data flash memory, 433, 868/916, or 310 MHz multi-channel radio transceiver, 38.4 kpbs radio, 500-1000 feet outdoor range (depending on versions) with a size of only 58 x 32 x 7 (mm).

Figure 1-2. Crossbow MICA2 mote (Source: http://www.xbow.com/products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf)

Usually it is run by TinyOS operating system and powered by 2 AA sized batteries. Clearly a device with this configuration cannot support security

mechanisms that require executing a large amount of instructions. In addition, a sensor network usually contains a large number of sensor nodes. The number of sensors in the network might directly affect the use of memory space of nodes participating in the network, because often they store pre-distributed secret keys, keying information, or the codes to calculate pairwise secret keys between nodes in the network. Node failure is another problem that could also affect the network severely. If a node is busy relatively longer than other nodes in the network (e.g., performing huge calculations related to security), it might lose its energy rapidly and can fail much sooner than the other less active nodes.

Table 1-1 presents the power consumption and resource data of two exemplary sensor node platforms; MICA2 and Tmote Mini mote (shown in Figure 1-3).

Table 1-1. Resources and energy consumption of two sensor platforms (a) From http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf

and (b) From http://www.sentilla.com/pdf/eol/Tmote_Mini_Datasheet.pdf

Properties	**MICA2 (a)**	**TMote Mini (b)**
RAM (KB)	4	10
Program Flash Memory (KB)	128	48
Maximum Data Rate (Kbps)	76.8	250
Energy Consumption: Receive (mW)	36.81	57.0
Energy Consumption: Transmit (mW)	87.90	57.0
Energy Consumption: Sleep (mW)	0.048	0.003

Nature of Work of WSN - Many applications of wireless sensor networks require deployment of sensors in remote, unattended, hostile, or hazardous areas. The sensors are often exposed to various types of adversaries and could be attacked physically. Even if they are deployed over a field, a passing vehicle can run over and physically damage them. An adversary can physically search and destroy the nodes [5]. Environmental conditions might also affect the performance of the sensors or can cause physical damage. All these unintentional or intentional events that can cause physical damage to a sensor are considered physical security issues. Sometimes physical attacks (like the capture or destruction of nodes) can cause several types of logical security attacks. A good deployment or management policy, tamper-proofing mechanisms of the physical package of the sensors, camouflaging, protective shields, or other available techniques [6] could be used for dealing with physical security threats in wireless sensor network. More discussions on these issues will be provided later in this chapter.

Figure 1-3. TMote Mini mote (Source: http://www.sentilla.com/pdf/eol/Tmote_Mini_Datasheet.pdf)

Use of Wireless Communications - Wireless technology is used for communications in a wireless sensor network. As with any other wireless

network, it is also prone to various types of threats related to the unreliable nature of wireless links like: undelivered packets, collisions of packets, latency, etc. Because of the broadcast nature of wireless channels, any adversary can even eavesdrop or passively listen to the transmissions of any legitimate node. In case of wired communication, the guided media would be well-protected by using various means and usually the end devices come with sufficient protective mechanisms. On the contrary, in wireless communication, because of its unguided medium and open nature, many types of attacks could be launched. In fact, many of the security threats in WSN exist because of the use of wireless technology for communications among the nodes.

1.1.2 Feasibility of Different Security Approaches in WSN

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback [7]. Over the past few decades, the more the dependency on network-provided information has increased, the more the risk has increased for secure transmission of information over the networks. To ensure various aspects of security (i.e., authenticity, integrity, privacy, etc.), diverse approaches like cryptography, steganography, physical layer security, etc. are used. In this section, we will examine which of the major security approaches can be viable for wireless sensor networks.

Cryptography - Most of the encryption-decryption techniques devised for traditional wired networks are not fit for direct use in wireless networks. As mentioned previously, WSNs consist of tiny low-cost devices which possess scarce processing, memory, and battery power resources. Applying any kind of encryption scheme requires transmission of extra bits, and thus requires extra processing, memory, and battery power which can impact the network's longevity. Encryption and decryption operations can also increase delay, jitter,

and packet loss in wireless sensor networks. Moreover, critical questions arise when applying an encryption-decryption scheme to WSN like: How the keys should be generated? How the keys should be disseminated? How the keys should be managed? What is the procedure to revoke the keys? How the keys could be assigned to a newly added sensor? As minimal (or no) human interaction is one of the fundamental features of WSN, it is also a crucial point to decide how the keys could be modified/refreshed from time to time for encryption. Adoption of pre-loaded keys or embedded keys might always not be the best solution. Overall, schemes that are based on cryptographic techniques must be lightweight so sensors can support them along with other programs, which are running and sharing the same resources.

Steganography - While cryptography aims at hiding the content of a message, steganography [8], [9] aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) [10]. The main objective of steganography is to modify the carrier in a way so that it is not perceptible and hence, looks ordinary. It hides the existence of the covert channel, and furthermore, if we want to send a secret data without sender information or want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography. Processing multimedia data (like audio, video) with the inadequate resources of the sensors is difficult. Steganography in WSNs remains as an open research issue that will not be solved until the sensors acquire enough capabilities to support extensive computations associated with it.

Physical Layer Secure Access - Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop), and hopping pattern (the sequence in which the frequencies from the available hopping set is used) could be used

with a little expense of memory, processing, and energy resources. Important point in physical layer secure access is the efficient design so that the hopping sequence is modified in less time than is required to discover it. One drawback for employing this is that both the sender and receiver should maintain a synchronized clock, therefore time synchronization in WSN [11] is another important research issue.

Considering all the basic security approaches, lightweight cryptography, logical or algorithmic schemes could be the best choice for WSN security. We must keep in mind that the higher the level of security of a WSN, the higher the amount of resources needed to support it.

1.2 Motivation and Report Contribution

1.2.1 Motivation and Problem Description

Because of the scarcity of resources of the tiny sensors, any kind of operation in a wireless sensor network must be done with special care. Resource efficiency should be given the highest priority in handling any aspect. Resources for a wireless sensor network are the computation power, storage capacity, energy level, and range of the wireless radio of the sensors. Sometimes, time could even be considered as a resource for WSN as timely data are required for deciding whether a particular sensor report should be taken into consideration while taking managerial decision. This is an interesting fact that employing high-level security needs utilization of considerable amount of available resources; again to make any security mechanism resource-efficient, number of tasks and communications, and amount of data need to be reduced. Hence, a trade off is needed between these two apparently conflicting objectives. To deal with these issues, one good

strategy is to consider ensuring security of the network from the very beginning state and then based on the acquired structure, carrying out the network's operation. This particular philosophy motivated us to write this report. We deal with the issue of handling security management in WSN in resource-efficient way so that we could get the maximum benefit with minimum exploitation of available resources.

1.2.2 Goals and Contributions

An important point is that the required level of security of any WSN often depends on the type of application. For a short-term military application, high level security is needed from the start up to the end. If resource efficiency can be ensured for such military application, the network lifetime could be maximized and more benefits could be achieved. For any other type of WSN application, a moderate level security could be enough but resource efficiency might be a crucial factor.

Before discussing the contributions of the report, we would like to clarify the term, 'level of security' used for our cases. As multiple factors are associated with the security issues in WSN, we indicate various facets of security when we use this term in the report. The issues include physical security of the sensors, topological security of the network (dense or sparse network), deployment security (the way the sensor deployments are handled), wireless communication security, and data security. If one aspect is weak, we consider that the level of security for that network is weak. Hence, 'high-level security' in our case means that all aspects of security are considered while taking any measure.

There is another way to view the issue of security in WSN known as holistic security. This brings forward the concept of layer-wise security in such type of network. Based on the very well-known OSI (Open Systems Interconnection)

reference model, we could think about ensuring security for each layer. Especially for wireless sensor networks, five layers are relevant; application layer, transport layer, network layer, link layer, and physical layer. Lack of security in any of these levels weakens the overall security of the network. We partially address this view of security in the report. However, full solution where different mechanisms could work in cooperation is still an open area of research which would take huge effort to develop.

Considering all these points, we propose our schemes in this report. Our mechanisms guarantee resource efficiency, good level of security, and prevent the inclusion of rogue nodes in the network from the bootstrapping state. In fact, most of the attacks against security mechanisms in wireless sensor network are launched due to the injection of false information either by compromised nodes residing in the network or by alien attackers. Hence, many attacks can be resisted by employing efficient schemes that can prevent the attackers from being included in the network from its formation stage. As sensors are equipped with constrained resources, our aim is to ensure efficient utilization of resources for our mechanisms. Both of our mechanisms can be integrated if any application needs that. For this case, using the first approach we can make sure that the entities we are dealing with are legitimate entities and no rogue node is included in our initially formed network. Then, on top of that, we could apply our secure routing protocol to provide both secure and energy-efficient data transmission in the network. Other routing protocols could also be used instead of our protocol. However, in that case, applying extra security mechanism for ensuring data transmission security might take more resources. It should be mentioned here that most of the other routing protocols do not consider any type of security as part of their working mechanisms. The consequent chapters deal with all these issues with explanations and detailed analyses of our approaches.

A good point to keep in mind is that no system is fool-proof. Hence, along

with the achievements our work, we also point out the drawbacks and possible disadvantages of our schemes. As the benefits are greater than the drawbacks, we believe that our work contributes significantly in the field of security in wireless sensor networks.

1.3 Outline of this Report

We have started the report with a brief introduction to WSN security. Subsequent chapters are organized as follows:

Chapter 2 explores major threats and attacks against wireless sensor networks, their detection, prevention, and attack countermeasures, key management issues, and secure routing issues. Also it presents a holistic view of security in WSN and some achievements and goals for research on WSN security. We have discussed all the security threats and attacks against WSN because we need to have clear idea about the vastness of security aspects in WSN. In fact, our mechanisms try to establish a defensive system so that many of these threats and attacks could be thwarted from the bootstrapping state of the network.

Chapter 2

Literature Review: Security Issues in Wireless Sensor Network

This chapter explores various types of threats and attacks against wireless sensor networks, possible countermeasures, and notable concepts on WSN security. We discuss these issues in detail because; most of the attacks are launched by using malicious nodes or with the help of malicious entities in the network. Hence, knowing the vastness of security aspects in WSN can give us a clear understanding about the difficulty of designing and developing efficient security systems for such type of network.

Several factors can be considered for categorizing the attacks in WSNs like; the approach of attack, target of the attack, position of attacker, role of attacker, etc. Overall, we can classify all of the known attacks into three basic types:

Type I

Attacks on the Basic Mechanism (e.g., attacks against routing in the network)

Attacks on the Security Mechanisms (e.g., against cryptographic scheme or against key management scheme)

Type II

Passive Attack – It typically means eavesdropping of data. In this case, the attacker passively listens to the transmitted data in the network and can use the collected information later for launching other types of attacks.

Active Attack – Any type of direct attack caused by an adversary. The attacker actively participates in the collection, modification, and fabrication of data. The information collected by passive attacks can be used for active attacks.

Type III

External Attack – In an external attack, an outsider is involved. These attacks can cause denial of service (DoS) situation, congestion, propagation of wrong routing information, etc. Typically external attacks can be resisted using firewalls, encryption mechanisms, and good security management policy.

Internal Attack – An Internal attack sometimes could be very harmful for the network as any node within the network works as an attacker in this case. Internal attack is performed by compromising node(s) in the network. Compromising a node means convincing a legitimate node to help the attacker or persuading a node in the network to work on behalf of the attacking entity. Often it is difficult to detect an internal attacker within the network that has a legitimate identity. Various kinds of authentication schemes, intrusion detection schemes, or membership verification schemes can be used for preventing it.

Other than these basic categories, several attacks are given formal names.

2.1 Denial of Service (DoS) Attack

Strictly speaking, we consider any kind of attempt of an adversary to disrupt, subvert, or destroy the network as a Denial of Service (DoS) attack. In reality, any kind of incident that diminishes, eliminates, or hinders the normal

activities of the network can cause a DoS situation. Some examples include hardware failures, software bugs, resource exhaustion, environmental conditions, or any type of complicated interaction of these factors. Note that, DoS (Denial of Service) is basically a given formal name of a particular condition of the network but when it occurs as a result of an intentional attempt of an adversary, it is called DoS attack. In general, 'Denial of Service (DoS)' is an umbrella term that can indicate many kinds of events in the network in which legitimate nodes are deprived of getting of expected services for some reasons (intentional attempts or unintentional incidents).

DoS attacks can mainly be categorized into three types:

(1) Consumption of scarce, limited, or non-renewable resources

(2) Destruction or alteration of configuration information

(3) Physical destruction or alteration of network resources

Among these types of DoS attacks, the first one is the most significant for wireless sensor networks as the sensors in the network suffer from the lack of resources. Other than these basic types, categorization of DoS attacks can be done according to the layers of the network architecture [12], [13]. An attacker can choose different targets at different layers to stop proper functioning of legitimate nodes so that they cannot get the services they are entitled to. Though it is quite difficult to know whether any particular DoS situation is caused intentionally or unintentionally, there are some common prevention and detection methods for each of the DoS attacks.

Let us now have a look at the DoS attacks in WSNs by layer:

DoS Attacks in Physical Layer

Jamming – Jamming means the deliberate interference with radio reception to

deny a target's use of a communication channel. For single-frequency networks, it is simple and effective, causing the jammed node unable to communicate or coordinate with others in the network. Due to their very nature, wireless sensor networks are probably the category of wireless networks most vulnerable to "radio channel jamming"-based Denial of Service (DoS) attacks [14]. Mainly two types of jamming could be possible; constant and sporadic. In case of constant jamming, attacker interferes with the signals of a legitimate node continuously for a certain period of time while in case of sporadic jamming, the attacker intermittently causes jamming. Sporadic jamming in the network is often more difficult to detect than detecting constant jamming. Some solutions to deal with jamming in WSN are proposed in [14], [15], and [16].

Tampering – Due to the unattended feature of wireless sensor networks, an attacker can physically damage/replace sensors, parts of computational and sensitive hardware, even can extract cryptographic keys to gain unrestricted access to higher communication layers. Tampering is actually any type of physical attack on sensors in the network. Success in tampering depends on: (a) how accurately and efficiently the designer considered the potential threats at design time, (b) resources available for design, construction, and test, (c) attacker's cleverness and determination

DoS Attacks in Link Layer

Collision – Adversaries may only need to induce a collision in one octet of a transmission to disrupt even a relatively longer packet. As the resources of the sensors are scarce, such loss could be significant in many cases. Also it is a great hurdle for acquiring timely and accurate data from the sensors. Unfortunately, in wireless networks, detection of a collision with a node's own transmission is difficult. Standard collision avoidance mechanisms also cannot help as they are cooperative by nature. An attacker simply can ignore the

avoidance protocol and transmit at the same time as the victim. One possible solution could be the use of error correction codes (ECC) but with the use of ECC, more processing and communication overheads are incurred.

Exhaustion – Battery exhaustion attack could be launched with repeated requests for using the channel. A naive link layer implementation could be a target for this type of attack. Feasible defense mechanisms against battery exhaustion caused by repeated transmissions could be the use of time division multiple access (TDMA) or rate limitation. Additional logic could also be developed to help these mechanisms.

Unfairness – Unfairness is a weaker form of DoS attack. This threat may not entirely prevent legitimate access to the channel, but could degrade service for real time MAC protocols. In fact, ensuring fairness in WSN is often viewed as a separate research issue. Use of small frames might be helpful in this case. However this would also incur some framing overhead.

DoS Attacks in Network Layer

Neglect and Greed – If a node drops packets or denies transmitting legitimate packets or if a node is very greedy to give undue priority to its own messages, these could be considered as 'neglect and greed'. Dynamic Source Routing (DSR) protocol or the protocols that are based on DSR are especially vulnerable to this type of attack. Use of multipath routing or redundant message transmission could be the solutions for handling such attacks. However, for WSNs these solutions might not be feasible. Instead, use of some other routing mechanisms could help.

Homing – Sometimes in WSNs, some nodes are given some special responsibilities like managing cryptographic keys, making use of acquired data, maintaining a local group, etc. Often the adversaries are attracted to these leader nodes and try to eavesdrop on their activities. In case of homing attack, the adversaries try to hamper the normal functioning of such types of leader nodes within a WSN. Different types of cryptographic schemes, algorithms, hiding management messages, etc. could be used for preventing homing attack.

Misdirection – It means simply directing the legitimate packets to the wrong path. A malicious insider can cause misdirection of traffic. Egress filtering, authorization and monitoring, or any kind of intrusion detection scheme (IDS) [17] could be used to prevent this type of DoS attack.

Blackhole – Blackhole (or Sinkhole) attack itself is one of the major attacks in WSN. We will discuss this attack in detail later in this chapter. However, when this attack causes any type of denial of service in the network, it is considered as a DoS attack in network layer.

Transport Layer DoS Attacks

Flooding – Protocols which must keep the states of both end-nodes are particularly vulnerable to this attack. It aims at memory exhaustion of the nodes by flooding of a great number of packets. Client puzzles or traceback mechanisms could be used to deal with such type of DoS attack.

Desynchronization – This attack means forging of packets during transmission. Existing connection between two endpoints could be effectively

disrupted by desynchronization. Any kind of authentication mechanism for the packets could be used to handle desynchronization attack.

DoS Attacks in Application Layer

External Stimuli - If the communications of nodes in a WSN are triggered by each occurred event, an application layer DoS attack could be launched by using some external physical stimuli. In such a case, the attacker uses the external stimuli to stimulate the nodes with huge number of events to be sent towards the base station. This attack is not effective when sensor readings are sent after making a gist or with regular intervals (for example, a clustered network where the clusterheads collect the raw data first and then send reports to the base station after certain intervals). On the other hand, some type of intrusion detection mechanism (IDM) can be used to detect the presence of any external entity in the network if a particular region creates a large volume of readings within a short period. An effective IDM can prevent the instant triggering of sensors by notifying the presence of intruder in the network and isolating it or ignoring it. However, such type of IDM is difficult to develop as sensor nodes cannot determine the legitimacy of a particular physical stimulus rather they only sense the event and get triggered.

PDoS - Path based DoS (PDoS) attack is another kind of application layer DoS attack. Each of the nodes in a path towards the base station needs to participate in the forwarding process of a particular packet containing sensor readings. If a large number of bogus packets are sent through a path towards the base station, it can keep the nodes busy, deny transmission of legitimate traffic by occupying network resources, and significantly drain the resources of the sensors. Use of various authentication mechanisms or replay protection mechanism could be the effective countermeasures against this type of attack.

Bogus Message During Reprogramming - A third type of application layer

attack could be launched if a WSN allows reprogramming of the network. Reprogramming of a sensor network may be needed for version control, scope selection, encoding-decoding, code dissemination, completion validation, code acquisition, switching to a new program, and/or for network management purpose [18]. In these cases, if the process of reprogramming is not secure enough, the attackers can actively cut off a portion of the network by using bogus messages. Good authentication mechanism for the whole process can resist this type of attack.

Other than these attacks, many other individually considered attacks like wormhole attack, hello flood attack, sybil attack etc. can also cause denial of service situation in the network. In fact, many of the methods of attacking and targets of attacks overlap with each other, but considering different circumstances, are given different tags and names. It should be clear that, any sort of intentional attempt that causes any sort of denial of service situation in the network is considered as DoS attack. As we will examine all other attacks in the rest of the chapter, here we conclude this section with the names of the major types of DoS attacks only.

2.2 Attacks on Information in Transit

The basic task of a sensor is to monitor the changes of some specific parameters (like temperature, sound, magnetism, light level, etc.) and to report those to the base station. The readings from the sensors could be transmitted using various methods. While in transit, the packets may be altered, spoofed, or vanished on the way (this type of attack could also be considered as network layer DoS attack when it resists a valid node from getting its expected service). As wireless communication is susceptible to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify, or fabricate packets.

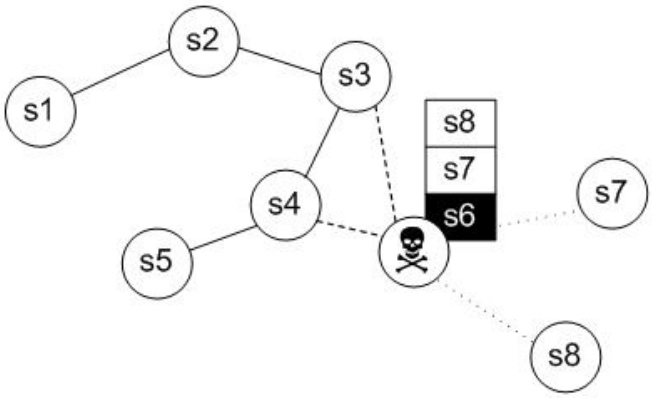

Figure 2-1. Conceptual view of a Sybil Attack. The node with id s6 is pretending to be three nodes at the same time (s6, s7, and s8), the nodes s3 and s4 do not have direct contacts with s7 and s8, so s6 can pretend to them as it is s7 or s8. Here, additional ids of s6 are called the 'Sybil nodes' (s7 and s8)

If the routing method does not have proper security measures, wrong information even can reach up to the base station and thus can influence the decision taken by the central authority. Such an event might be extremely dangerous for a military reconnaissance scenario which could lead to taking disastrous military decisions. As sensor nodes typically have short range of transmission and scarce resources, an attacker with adequate processing power and larger communication range can attack several sensors at the same time to modify the actual information during transmission. Among several works, a good approach to tackle this and to filter out falsely injected data in sensor networks is presented in [19].

2.3 Sybil Attack

Sometimes the sensors in a wireless sensor network might need to work together to accomplish a task, hence the management policy of the network can

use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node at the same time using the identities of other legitimate nodes. This type of attack is called a Sybil attack [20]. The malicious device's additional identities are called the Sybil nodes. Sybil attack tries to degrade the integrity of data, level of security, and resource utilization that a distributed algorithm targets to achieve. This type of attack can be performed for downgrading the performances of distributed storage, routing mechanism, data aggregation, voting, fair resource allocation, and misbehavior detection mechanisms. A conceptual view of Sybil attack is shown in Figure 2-1. Basically, any peer-to-peer network (any kind of wireless ad hoc network) is vulnerable to Sybil attack. Newsome et al. [21] presented a taxonomy of sybil attacks in WSN based on three orthogonal dimensions.

Dimension I

Direct Communication – In this case, Sybil nodes directly communicate with the legitimate nodes. When a legitimate node sends message to a Sybil node, malicious device listens to the message. In the same way, messages sent from the Sybil nodes are actually sent from the malicious device.

Indirect Communication – In this case, the legitimate nodes cannot directly communicate with the Sybil nodes rather a malicious device convinces them that it can reach to the Sybil nodes. Any message sent by a legitimate node to a Sybil node is routed through the malicious node which can do anything (modification, fabrication, dropping, etc.) with the received messages.

Dimension II

Identities used for the Sybil nodes could be obtained in one of two ways:

Fabricated Identities – Attacker can simply generate a fake identity supported by the network and perform Sybil attack.

Stolen Identities – Attacker in this case steals the identities of the legitimate nodes and uses those for launching attacks.

Dimension III

The identities of the Sybil nodes could be used in two ways:

Simultaneous – The malicious node or the attacker can pretend to have multiple identities at the same time (as shown in Figure 2-1).

Non-simultaneous – The attacker can somehow obtain a large number of valid identities but, instead of using all the identities at the same time, it can use those one after another in different time slots.

One advantage for WSN to face Sybil attack is that, it can have some sort of centralized entity (base station or cluster head) in the network. Hence, this attack could be prevented using efficient protocols. Douceur [20] showed that, without a logically centralized authority, sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of sybil nodes in a network is not so easy. Some of the recently proposed detection and prevention mechanisms could be found in [22], [23], [24], [25], and [26].

2.4 Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole [27] to attract all the traffic in the network. Especially in a flooding based protocol, the attacker listens to the route request and then replies to the target node saying that it has a high quality or shortest path to the base station. A victim node is thus lured to select

it as a forwarder of its packets. Once the malicious device is able to insert itself between the communicating entities (between the base station and sensor node), it is able to do whatever it wishes with the packets that pass through it.

Figure 2-2. Conceptual view of a Blackhole/Sinkhole Attack. The attacker advertises high quality link through it which tempts s3, s4, s6, and s7 to select itself as a forwarding node for their packets. In the figure, B is the base station and the large gray circle is the attacker's radio range

The blackhole (i.e., malicious node or the attacker) can drop the packets, selectively forward those to the base station or to the next node, or even can change the content of the packets. This type of attack could be very harmful for those nodes that are considerably far from the base station. We should keep in mind that blackhole attack and sinkhole attack are basically the same attack but these two terms are often used interchangeably. As mentioned earlier, this attack can cause DoS in the network and thus could be considered as one type of DoS attack. Figure 2-2 shows a conceptual view of a blackhole/sinkhole attack. Some recent works addressing this attack and possible solutions to deal with it are [28], [29], [30], [31], [32], [33], [34], and [35].

2.5 Hello Flood Attack

Hello flood Attack was first detected and introduced by Karlof and Wagnor in [36]. This attack uses HELLO packets as a weapon to convince the sensors in the network. Many protocols require broadcasting of HELLO packets for neighbor discovery. In this case, a node receiving such a packet may assume that it is within (normal) radio range of the sender node. This assumption could be exploited by an attacker. An attacker with a large radio transmission range (termed as a laptop-class attacker in [36]) and enough processing power can send HELLO packets to a large number of sensors in the network. Thus the sensors could be persuaded that the adversary is their neighbor.

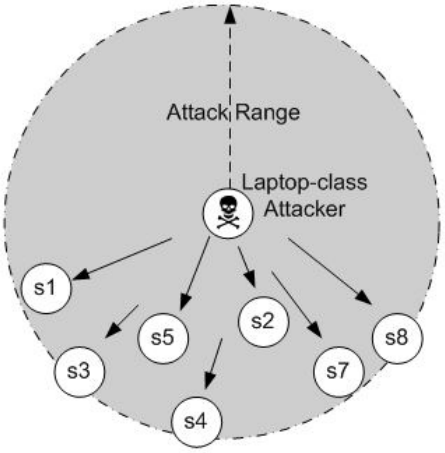

Figure 2-3. Hello flood Attack. A Laptop-class attacker (attacker with large radio range) is transmitting the HELLO packets and pretending to be a neighbor of all other legitimate nodes within its radio range

As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know it as their neighbor. A conceptual picture of hello flood attack is presented in Figure 2-3. Possible countermeasures to handle hello flood attack could be the use of bidirectional verification of links before using them, multipath routing, use of multiple base stations [37], or any kind of lightweight packet authentication scheme.

2.6 Wormhole Attack

Wormhole attack is a very critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location [38]. The tunneling or retransmission of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks because this is possible even if the attacker has not compromised any node, and even if all communications provide authenticity and confidentiality. It could be performed even at the initial phase when the sensors start discovering the neighborhood information.

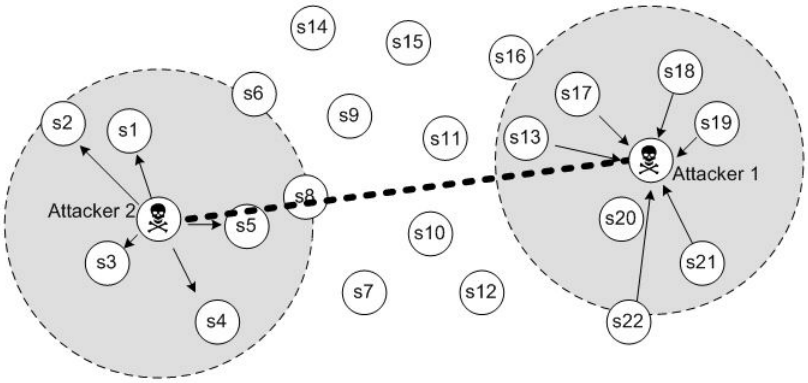

Figure 2-4. Wormhole attack. Two attackers have created a dedicated tunnel between them and are attracting traffic

Figure 2-4 shows a graphical representation of wormhole attack. In the figure, two adversaries are communicating with each other through a direct and dedicated channel by using wired link or additional RF (radio-frequency) transceivers with longer transmission range. The route via the wormhole looks like an attractive path to the legitimate sensor nodes because it generally offers less number of hops and less delay than other normal routing paths. While relaying packets, the adversaries can arbitrarily drop the packets. Therefore data communications through the wormhole suffer from severe performance

degradation. In a recently published work, Sharif and Leckie propose three new variants of wormhole attacks namely Energy Depleting Wormhole Attack (EDWA), Indirect Blackhole Attack (IBA), and Targeted Energy Depleting Wormhole Attack (TEDWA). Interested readers are suggested to read [39].

Several works tried to defend against this attack by detection of intruder nodes in the network. Some of them are [28], [33], [40], [41], [42], [43], [44], [45], [46], and [47]. Other than these works, [48] proposes an approach to deal with wormhole attacks using directional antennas, which is often not feasible for sensor networks.

So far, we have talked about various security threats and attacks in wireless sensor networks. Most of these attacks can be tackled by using proper cryptographic mechanisms. If the node authentication method is robust and messages in the network are made illegible to the outside entities, many security problems are eventually resolved or just need a little add-on with the defense mechanism. For utilizing any kind of cryptographic operation in the network, key management is a fundamental issue to deal with. Given the constrained resources of the sensors and the special characteristics of wireless sensor networks, key management in WSN is considered to be a very challenging topic and a hot research issue. Efficient mechanisms and management policies are needed to determine how the keys in such a network would be generated, stored, used, manipulated, renewed, or revoked. In the next section, we will try to get some insights on these issues.

Table 2-1. Major attacks and threats against WSN at a glance

Denial of Service Attack	DoS Attacks in Physical Layer
	DoS Attacks in Link Layer
	DoS Attacks in Network Layer

	Transport Layer DoS Attacks	
	DoS Attacks in Application Layer	
Attacks on Information in Transit		
Sybil Attack	Dimension I	Direct Communication
		Indirect Communication
	Dimension II	Fabricated Identities
		Stolen Identities
	Dimension III	Simultaneous
		Non-simultaneous
Blackhole/Sinkhole Attack		
Wormhole Attack		

2.7 Key Management Issues in WSN

Primary goal of key management is to set up secure links among the neighboring nodes in the network at the formation phase. Some of the major challenges any kind of key management mechanism faces are:

(i) Unknown scalability of the network. It means that if there are n number of nodes initially in the network, n´ more nodes could be added to it later. The key management scheme must consider the tactics to handle the addition of

nodes in the network.

(ii) Unknown topological distribution of sensors in the network. As the topological information of the sensors are often very difficult to obtain and not known in prior in most of the cases, the key management scheme must distribute keys or keying information in such a way that the neighbor nodes could communicate securely with each other.

(iii) Limited available resources of the sensors. Like any other mechanism, this is a great hurdle that the key management scheme must confront with.

(iv) What if the nodes in the network are captured by adversaries? The key revocation mechanism should ensure that the captured keys cannot be used further in the network and still the network should be able to keep functioning with proper level of security.

(v) Re-keying. If there is any re-keying mechanism in the management scheme, how to generate or distribute the new keys among the already deployed sensors in the network?

There are mainly three kinds of approaches for key management in wireless sensor network:

- Key Pre-Distribution
- Key Management Based on Public Key
- Key Management Based on Online Server

Key Pre-Distribution

In case of key pre-distribution schemes, keys or the keying materials are delivered to all sensor nodes prior to their deployment. Keying materials are partial information of the keys that could be used by the nodes to derive keys

for node-to-node secure communications. Among all the key management approaches, key pre-distribution seems to be the most feasible solution. This is because; most of the operations in this approach can be done prior to the deployment of the network.

For key pre-distribution, we mainly consider two phases of operations; initialization phase and network formation phase. In the initialization phase, most of the planning and computations are done so that the sensors could get relief of the heavy computational burdens. In the formation phase, the sensors establish secure links among themselves based on the pre-stored information in their memories.

There are mainly three approaches of key pre-distribution:

System key pre-distribution – Same key k is stored in each sensor. k could also be used for deriving other keys for secure communications among the sensors. The advantage of this approach is the use of little memory to store the key. The drawbacks are little resilience and weak authentication.

Trivial key pre-distribution – Distinct pairwise keys $k_{i,j}$ are stored for each pair of nodes s_i and s_j. The two nodes contact with each other to derive the pairwise key for further secure communications. The advantage of this approach is greater resilience and strength of authentication. However, this approach is not scalable and in this case, it is hard to handle the addition of new sensors in the network.

Random key pre-distribution – In this approach, a number of random keys (say w keys) from a key pool is stored in the sensors. Any two nodes in the network may share a key with probability p. The advantage of this type of scheme is the resiliency and support for addition of new sensors in the network. On the other hand, the drawbacks are the lose node authentication and possibility of not finding a common key even among the neighboring nodes. One of the legendary works on random key pre-distribution, known as the

basic scheme was proposed by Eschenauer and Gligor [49]. The basic scheme is one of the early works which opened the door for further research on various aspects of key management in this type of network.

Key Management Based on Public-Key

Public key based schemes use asymmetric keys for encryption and decryption operations. There are some well-established public-key based schemes like Diffie-Hellman, Digital Signature Standard, ElGamal, Elliptic Curve Cryptography (ECC), RSA, etc. [50]. But the reality is, public key cryptography (PKC) based schemes are often not directly applicable for wireless sensor networks. As mentioned earlier, the limitation of resources of the sensors is the major hurdle for using these mechanisms. Also the need for a certificate authority or a trusted middle-man, unknown topology of the network, and random deployment of sensors often make their use more difficult. In spite of the existence of these barriers, the existing PKC schemes could somehow be modified for making them suitable for use in the sensors. Often the number of operations is reduced to make the PKC schemes a bit lightweight. Though in the early days, the researchers thought that the PKC schemes are in all the ways inappropriate for WSN, some recent works have shown that some lightweight versions of these schemes might be very effective for high-security demanding applications. The works like [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], and [62] have presented some success stories and gains regarding using public key based security mechanisms and key management in WSN.

Key Management Based on Online Server

In this approach, an online server provides the necessary keys to the sensors

for communications among themselves. The key could be provided by the base station or by the group leaders (sometimes called as cluster heads) in the network. However, this approach is not as efficient as the key pre-distribution approach as in this case, the special nodes must have relatively more memory, processing power, and energy than those of the ordinary sensors in the network. Also, the special nodes should be well-dispersed in the network so that they can cover the whole network for providing the keys with minimum effort. Maintaining security during the transmission of keys also requires some other supporting mechanisms or some trust-based approach. Overall, most of the researchers agree that this approach in most of the scenarios, not a good solution for managing keys in this type of network.

Some of the recent and notable works on key management in sensor networks are [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], and [81]. Readers are encouraged to go through these for gaining in-depth knowledge on key management in wireless sensor networks. Other than these works, a recent survey on the key management schemes in WSN is presented in [82].

2.8 Secure Routing and Physical Security Issues

Basically, secure routing is not a separate issue than that we have discussed so far. If we have an efficient key management scheme with a supporting security infrastructure, this issue is easily solved. In that case, the whole thing reduces to the task of verifying who is communicating with whom and through whom. A number of routing protocols are proposed for wireless sensor networks (for further reading, [83] and [84] are suggested to the interested readers). However, the key point is that most of the routing protocols have overlooked the issue of security at their design phase. Sometimes it is quite impossible to fit a good security mechanism with a good routing protocol.

If the operational method of a routing protocol does not support a particular security mechanism, we need to choose any other suitable security approach for that one. In such a case, often the suitable security solution might not be the best solution or might not at all help for secure routing using that particular protocol. A routing protocol may focus on saving energy resources of the sensors, but if a security mechanism is added to it, it might not hold its major point of advantage or could even turn into an energy-consuming routing protocol. Therefore, it is better to consider the security issues at the design phase of any routing protocol. If the structural design and communication methods of the routing protocol allow the security solutions to run side-by-side or on top of it, then it could be beneficial for secure routing as well as for handling almost all types of threats and attacks in WSN. Nonetheless, it should be noted that a single solution cannot solve all the problems at the same time. Instead, based on the application requirements and network settings, the strategy of routing and security should be set. Often we need to consider some trade offs among some parameters like security, QoS (Quality of Service), latency, packet loss, etc.

In one of the prominent works on secure routing in wireless sensor networks, Karlof and Wagner [36] noted that: "One aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation. In more conventional networks, a secure routing protocol is typically only required to guarantee message availability. Message integrity, authenticity, and confidentiality are handled at a higher layer by an end-to-end security mechanism such as SSH or SSL. End-to-end security is possible in more conventional networks because it is neither necessary nor desirable for intermediate routers to have access to the content of messages. However, in sensor networks, in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. Link layer security mechanisms can help mediate some of the

resulting vulnerabilities, but it is not enough: we will now require much more from our routing protocols, and they must be designed with this in mind."

In general, for secure routing in wireless sensor networks, the following points could be considered:

- Multipath routing can help for introducing some sort of security.

- Use of symmetric key cryptography can reduce the processing overhead.

- The routing protocols should be intrusion tolerant and should be able to keep on functioning at least up to a certain level so that the overall network operations are not hampered in case of the presence of intruders.

- As involvement of security mechanisms can increase the overheads of the protocol, the overall design should be kept as simple as possible.

- Any broken routing path should not hamper the functions of the associated security mechanisms. The working method of the protocol should allow finding an alternate path to the destination within a minimum interval.

Earlier we have introduced the types of physical attacks in WSN in brief. In this section, we will have a closer look at the physical security issues in wireless sensor networks. We know that the sensors in the network could be physically reached by adversaries because of the network's unattended nature. There are several ways to protect a sensor network from the physical attacks.

- The most suitable way to tackle this is the concept of self-destruction. In this case, a sensor detects a physical attack and quickly deletes all of its hidden information to become non-functional. For a large-scale sensor network, this could be a feasible solution as their might be several backups of the sensors' data, cryptographic keys, codes, and other secret information. Also if a part of the network is attacked, the sensors in other parts can be ready to destroy themselves before getting captured. Though this sort of self-destruction mechanism is expensive to incorporate with the sensor's physical package, it is

not impossible.

- An alternate solution could be using a mechanism where each sensor monitors the status of its neighbors. Any suspicious behavior of a neighbor for a certain period of time might trigger a warning. Consequently, other neighbors can get ready for hiding all of their secret information.

- Analyzing the deployment policy and detailed mapping of the network could also be effective for reducing the probability of physical attacks. However, in many applications, such kind of thorough study might not be possible.

- Camouflaging of sensors could be efficient in some deployment scenarios. Say for example, a wireless sensor network is to be deployed over a rocky hilly area. In that case, the sensors could be colored like rocks or could be given the shapes of rocks (with some outer coverings!), which can make the task of physically locating them more difficult.

- Sensors might have some sort of protective shields that can save the internal hardware from external pressure or from other environmental conditions.

- However, applying any of these approaches depends on the deployment budget and requirements of the application. Some of the recent works on physical security issues in wireless sensor networks can be found in [5], [6], [85], and [86].

2.9 Research Challenges

With the sophistication of various communication protocols and rapid advancements of Micro-Electro-Mechanical Systems (MEMS) technologies [87], sensors are gaining more resources and capabilities with which many barriers of security could be surmounted. In spite of the previous advancements and those that are coming in the near future, some issues regarding security in

WSN could still pose great challenges. In this section, we will talk about those issues and will try to visualize the future so that the research works on security in WSN may get a proper direction towards devising realistic solutions.

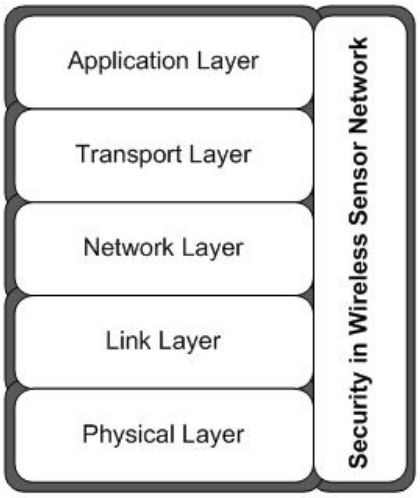

Figure 2-5. Holistic view of security in WSN

2.9.1 Holistic Approach to Security in WSN

A holistic approach (Figure 2-5) aims at improving the performance of wireless sensor networks with respect to security, longevity, and connectivity under changing environmental conditions. This approach of security concerns about involving all the operational layers for ensuring total security in the network. When talking about layering concepts, it should be mentioned that the security in network layer is mainly concerned about authentication, availability of routing information, and integrity of information, the data link layer is concerned mainly about data confidentiality and data freshness, and the physical layer is concerned about tamper-resistance.

Holistic approach tries to lead to a single architecture so that different security mechanisms can work in tandem for different layers. Some key principles of

holistic approach are:

In a given network, the cost for ensuring security should not surpass the assessed security risk at a specific time.

If there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation, if some of the sensors in the network are compromised, out of order, or captured by the enemy.

The security measures should be developed to work in a decentralized fashion.

Considering all types of security threats and attacks in WSN, we can understand that for this type of network, a single security solution for a single layer cannot be considered as a reasonable solution. It is better to employ a holistic approach so that all facets of the network could be made secure at the same time. As an example, if a WSN has very good security solutions for almost all the layers but physically the network is vulnerable, we cannot guarantee that the total security of the network is ensured. In such a case, any adversary can go and pick up the sensors from the field, extract the cryptographic keys, can use jamming for causing physical layer DoS attacks, destroy the sensors, and so on. Though physical security is often not possible to ensure for WSNs, at least the overall system must allow a graceful degradation of the network's operation when it is attacked. However, designing and developing such type of efficient security architecture and management policy remain as an open challenge. At least we can hope that with the advancements of technological capabilities of sensors, this task will become a bit easier in the future.

Figure 2-6. Imote2 node (Source: http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/Imote2_Datasheet.pdf)

2.9.2 Achievements and Goals

Today, the limitation of resources of the sensors is considered as the primary obstacle for applying robust security mechanisms. In future, this barrier might totally be vanished or might be reduced by significant extent. We might see sensors capable of handling even the heavy computations associated with public key cryptography schemes (like RSA, SHA-1, etc.) without any reduced operation. Say for example, one of the latest advanced wireless sensor platforms, Imote2 (shown in Figure 2-6) [88] is built with the low power PXA271 XScale processor at 13-416MHz and it integrates an 802.15.4 radio (CC2420) with a built-in 2.4GHz antenna. Imote2 has 256kB SRAM, 32MB FLASH, and 32MB SDRAM. It is a modular stackable platform and can be expanded with extension boards to customize the system to a specific application. Through the extension board connectors, sensor boards can provide specific analog or digital interfaces. A battery board is provided to supply system power, or even it can be powered via the integrated USB

interface. All these features make it a very powerful sensor node compared to its predecessors. The rechargeable feature of the sensor's battery opens the door to overcome the problem of constrained and non-renewable energy.

Considering today's achievements, it is reasonable to assume that some years later we could even see sensors with much higher configurations with the same tiny size! If it becomes true, some interesting questions may arise. What will be the case if these tiny devices get the capabilities like high configuration computers? Will we be able to run classic security schemes that require heavy computations? If so, will all the works done so far be meaningless? The answer to all of these questions is; "No work will be thrown away even if the sensors achieve very high configurations". Basically the researchers have been working on the fact that, given such low-configuration devices, how best level of security can be provided for the network. Yes, in future the sensors might get more capabilities keeping even today's physical size, but even then the devices with current specifications could remain as low-cost alternatives. Also, some other tiny devices might have such limited resources. It is also reasonable to think that the sensors with current specifications might become much smaller in physical size. If it becomes true, in that case, reduction of physical size would ultimately increase the level of physical security of these devices. In fact, reduced size of sensors would make them more physically secure in the hostile deployment areas as a relatively smaller object is harder to notice! Hence, the major point is, no matter how much capabilities a sensor node attains in future, the research works done with today's given limitations (like MICA2's specifications) will still be useful for use for the devices with such capabilities. As a whole, the research area will still remain challenging.

In future we might also see wide-spread use of wireless multimedia sensor networks [89], [90] for various security applications like; distributed vision, tracking, and monitoring applications. At that time, processing multimedia data might become a little bit easier. However, when issues like QoS (Quality

of Service) and latency are involved with this, the challenge is likely to remain for finding efficient solutions. In fact, ensuring a good level of QoS and a good level of security at the same time is always very difficult and often contradictory! Not only for sensor networks but also for other types of networks this statement is true. This is because, any sort of security operation requires some processing time. If the level of security is increased, the processing delay also increases causing degradation of quality of service. For real-time multimedia applications (if at all possible using WSNs or if at all required!), this challenge will remain for a long time.

Some of the recent works show that, in future some applications might need to handle multiple types of data within the same network [91]. The development of sensors like ExScal motes [92], [93] has already opened the door for further research on heterogeneous applications using homogenous multi-purpose nodes. The heterogeneous data generated from such multipurpose nodes might have different levels of security based on their priorities. Handling these heterogeneous data with different security levels could also be an interesting topic for research in the near future.

Viewing Angle 1	
Key Management	YES
Secure Routing	YES
Secure Services	YES
Intrusion Detection Systems (IDS)	NO
Viewing Angle 2	
Physical security	NO
Deployment security (sparse or dense, etc.)	YES
Topological security (cluster, hierarchy, tree, etc.)	YES
Wireless communication security	YES
Data security	YES
Holistic security based on various layers	Not considered but mentioned

Bibliography

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E., "Wireless Sensor Networks: A Survey," Computer Communications, Volume 38, 2002, pp. 393–422.

[2] Pathan, A.-S. K., Lee, H.-W., and Hong, C. S., "Security in Wireless Sensor Networks: Issues and Challenges," Proceedings of the 8th IEEE ICACT 2006, Volume II, Phoenix Park, Korea, 20-22 February 2006, pp. 1043-1048.

[3] Hämäläinen, P., Kuorilehto, M., Alho, T., Hännikäinen, M., and Hämäläinen, T. D. (2006), "Security in Wireless Sensor Networks: Considerations and Experiments," SAMOS 2006, LNCS 4017, Springer-Verlag, pp. 167–177.

[4] Xbow Sensor Networks, Available at: http://www.xbow.com/

[5] Gu, W., Wang, X., Chellappan, S., Xuan, D., and Lai, T.H., "Defending Against Search-Based Physical Attacks in Sensor Networks," 2005 IEEE International Mobile Adhoc and Sensor Systems Conference (IEEE MASS 2005).

[6] Becher A., Benenson Z., and Dornseif, M., "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks," SPC 2006, LNCS 3934, Springer-Verlag 2006, pp. 104–118.

[7] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks," CADIP Research Symposium, available at http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

[8] Kurak, C. and McHugh, J., "A Cautionary Note on Image Downgrading in Computer Security Applications," Proc. of the 8th Computer Security Applications Conference, 1992, pp. 153–159.

[9] Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography," Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, pp. 41–50.

[10] Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H. W., "Steganalysis on BPCS Steganography," Pacific Rim Workshop on Digital Steganography (STEG'03), Japan, 2003.

[11] Römer, K., Blum, P., and Meier, L., "Time Synchronization and Calibration in Wireless Sensor Networks," Handbook of Sensor Networks:

Algorithms and Architectures (Ivan Stojmenovic Ed.), John Wiley & Sons, ISBN 0-471-68472-4, pp. 199–237.

[12] Wood, A. D. and Stankovic, J. A., "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks," Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (edited by Ilyas, M. and Mahgoub, I.), CRC Press, 2004.

[13] Raymond, D. R. & Midkiff, S. F. (2008), "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, January-March 2008, pp 74-81.

[14] Čagalj, M., Čapkun, S., and Hubaux, J.-P., "Wormhole-Based Antijamming Techniques in Sensor Networks," IEEE Transactions on Mobile Computing, Vol. 6, No. 1, 2007, pp. 100–114.

[15] Wood, A. D., Stankovic, J. A., and Son, S. H., "Jam: A Jammed-Area Mapping Service for Sensor Networks," Proc. of the 24th IEEE Real-time Systems Symposium, 2003, pp. 54–62.

[16] Alnifie, G. and Simon, R., "A Multi-Channel Defense Against Jamming Attacks in Wireless Sensor Networks," Proc. of ACM Q2SWinet'07, Crete Island, Greece, 2007, pp. 95–104.

[17] Chen, H., Han, P., Zhou, X., and Gao, C., "Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks," PAISI 2007, LNCS 4430, Springer-Verlag 2007, pp. 105–116.

[18] Wang, Q., Zhu, Y., & Cheng, L., "Reprogramming Wireless Sensor Networks: Challenges and Approaches," IEEE Network, May/June 2006, pp 48-55

[19] Ye, F., Luo, H., Lu, S. and Zhang, L, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE Journal on Selected Areas in Communications, 23(4), April 2005, pp. 839-850.

[20] Douceur, J. R. "The Sybil Attack," IPTPS 2002, LNCS 2429, Springer-Verlag 2002, pp. 251–260.

[21] Newsome, J., Shi, E., Song, D., and Perrig, A., "The Sybil Attack in Sensor Networks: Analysis & Defense," Proc. of ACM IPSN'04, California, USA, 2004, pp. 259–268.

[22] Zhang, Q., Wang, P., Reeves, D.S., and Ning, P., "Defending against Sybil attacks in sensor networks," Proc. of the 25th IEEE International

Conference on Distributed Computing Systems Workshops, 2005, pp. 185–191.

[23] Mukhopadhyay, D. and Saha, I., "Location Verification Based Defense Against Sybil Attack in Sensor Networks," ICDCN 2006, LNCS 4308, Springer-Verlag 2006, pp. 509–521.

[24] Yu, H., Kaminsky, M., Gibbons, P. B., and Flaxman, A., "SybilGuard: Defending Against Sybil Attacks via Social Networks," Proc. of ACM SIGCOMM 2006, pp. 267–278.

[25] Jiangtao, W., Geng, Y., Yuan, S., and Shengshou, C., "Sybil Attack Detection Based on RSSI for Wireless Sensor Network," Proc. of WiCom 2007, pp. 2684–2687.

[26] Tanachaiwiwat, S. and Helmy, A., "Correlation Analysis for Alleviating Effects of Inserted Data in Wireless Sensor Networks," Proc. of MobiQuitous 2005, pp. 97–108.

[27] Ahmed, N., Kanhere, S., and Jha, S., "The Holes Problem in Wireless Sensor Networks: A survey," ACM SIGMOBILE Mobile Computing and Communications Review, V.9 N.2, 2005, pp. 4–18.

[28] Pirzada, A. A. and McDonald, C., "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks," Proc. of International Workshop on Wireless Ad Hoc Networks 2005, London.

[29] Karakehayov, Z., "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Proc. of REALWSN 2005, Stockholm, Sweden.

[30] Yin, J. and Madria, S.K., "A Hierarchical Secure Routing Protocol against Black Hole Attacks in Sensor Networks," Proc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Volume 1, 2006, pp. 376–383.

[31] Ramaswami, S. S. and Upadhyaya, S., "Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing," Proc. of the 2006 IEEE Workshop on Information Assurance, NY, USA, pp. 253–260.

[32] Ngai, E. C. H., Liu, J., and Lyu, M. R., "An Efficient Intruder Detection Algorithm Against Sinkhole Attacks in Wireless Sensor Networks," Computer Commun., Vol. 30, 2007, pp. 2353–2364.

[33] Nahas, H. A., Deogun, J. S., and Manley, E. D., "Proactive Mitigation of Impact of Wormholes and Sinkholes on Routing Security in Energy-Efficient Wireless Sensor Networks," Wireless Networks, Springer Netherlands, 2007.

[34] Demirbas, M. and Song, Y., "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," Proc. of IEEE WoWMoM 2006, pp. 564–570.

[35] Krontiris, I., Dimitriou, T., Giannetsos, T., and Mpasoukos, M., "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks," 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors'07), Wroclaw, Poland.

[36] Karlof, C. and Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, 2003, pp. 293-315.

[37] Hamid, M. A., Mamun-Or-Rashid, M., and Hong, C. S., "Routing Security in Sensor Network: HELLO Flood Attack and Defense," Proc. of IEEE ICNEWS, Dhaka, Bangladesh, 2006, pp. 77–81.

[38] Hu, Y. C., Perrig, A., and Johnson, D. B., "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, 2006, pp. 370–380.

[39] Sharif, W. and Leckie, C., "New Variants of Wormhole Attacks for Sensor Networks," Proceedings of the Australian Telecommunication Networks and Applications Conference, Melbourne, Australia, 2006, pp. 26–30.

[40] Hu, Y.-C., Perrig, A., and Johnson, D. B., "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. of INFOCOM 2003, Vol. 3, pp. 1976–1986.

[41] Buttyán, L., Dóra, L., and Vajda, I., "Statistical Wormhole Detection in Sensor Networks," ESAS 2005, LNCS 3813, Springer-Verlag 2005, pp. 128–141.

[42] Alzaid, H., Abanmi, S., Kanhere, S., and Chou, C. T. Detecting Wormhole Attacks in Wireless Sensor Networks. Technical Report, Computer Science and Engineering School, The Network Research Laboratory, University of New South Wales, 2006.

[43] Maheshwari, R., Gao, J., and Das, S. R., "Detecting Wormhole Attacks in Wireless Sensor Networks Using Connectivity Information," Proc. of INFOCOM 2007, pp. 107–115.

[44] Khalil, I., Bagchi, S., and Shroff, N. B., "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks," Ad Hoc Networks, Volume 6, Issue 3, 2008, pp. 344–362.

[45] Yun, J.-H., Kim, I.-H., Lim, J.-H., and Seo, S.-W., "WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks," ICUCT'06, LNCS 4412, Springer-Verlag, pp. 200–209.

[46] Poovendran, R. and Lazos, L., "A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks," Wireless Network, Vol. 13, Springer, 2007, pp. 27–59.

[47] Xu, Y., Chen, G., Ford, J., and Makedon, F. S., "Distributed Wormhole Detection in Wireless Sensor Networks," Book Series of Critical Infrastructure Protection: Issues and Solutions, Springer, Boston, 2007.

[48] Hu, L. and Evans, D., "Using Directional Antennas to Prevent Wormhole Attacks," Proc. of the 11th Network and Distributed System Security Symposium, 2003, pp. 131–141.

[49] Eschenauer, L. and Gligor, V. D., "A Key-Management Scheme for Distributed Sensor Networks," Proc. of the 9th ACM conference on Computer and Communications, USA, 2002, pp. 41–47.

[50] Rhee, M. Y., Internet Security: Cryptographic Principles, Algorithms and Protocols, WILEY, 2003.

[51] Malan, D.J., Welsh, M., and Smith, M.D., "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," Proc. of IEEE SECON, 2004, pp. 71–80.

[52] Watro, R., Kong, D., Cuti, S.-f., Gardiner, C., Lynn, C. and Kruus, P., "TinyPK: Securing Sensor Networks with Public Key Technology," Proc. of ACM SASN, 2004, pp. 59–64.

[53] Du, W., Wang, R., and Ning, P., "An Efficient Scheme for Authenticating Public Keys in Sensor Networks," Proc. of ACM MobiHoc'05, Illinois, USA, 2005, pp. 58–67.

[54] Gaubatz, G., Kaps, J., and Sunar, B., "Public Keys Cryptography in Sensor Networks -- Revisited," ESAS 2004, LNCS 3313, Springer-Verlag 2005, pp. 2–18.

[55] Gaubatz, G., Kaps, J.-P., Öztürk, E., and Sunar, B., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2005), pp. 146–150.

[56] Blaß, E.-O. and Zitterbart, M., "Towards Acceptable Public-Key Encryption in Sensor Networks," Proc. of ACM 2nd International Workshop on Ubiquitous Computing, 2005, pp. 88–93.

[57] Jing, Q., Hu, J., and Chen, Z., "C4W: An Energy Efficient Public Key Cryptosystem for Large-Scale Wireless Sensor Networks," Proc. of IEEE MASS 2006, pp. 827–832.

[58] Nyang D. and Mohaisen A., "Cooperative Public Key Authentication Protocol in Wireless Sensor Network," UIC 2006, LNCS 4159, Springer-Verlag 2006, pp. 864–873.

[59] Mykletun, E., Girao, J., and Westhoff, D., "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proc. of IEEE International Conference on Communications (ICC'06), Volume 5, 2006, pp. 2288–2295.

[60] Arazi, O., Elhanany, I., Rose, D., Qi, H., and Arazi, B., "Self-Certified Public Key Generation on the Intel Mote 2 Sensor Network Platform," Proc. of the 2nd IEEE Workshop on Wireless Mesh Networks (WiMesh 2006), pp. 118–120.

[61] Arazi, O., Qi, H., and Rose, D., "Public Key Cryptographic Method for Denial of Service Mitigation in Wireless Sensor Networks," Proc. of the 4th IEEE SECON 2007, pp. 51–59.

[62] Pathan, A.-S. K., Ryu, J. H., Haque, M. M., and Hong, C. S., "Security Management in Wireless Sensor Networks with a Public Key Based Scheme," APNOMS 2007, LNCS 4773, Springer-Verlag 2007, pp. 503–506.

[63] Pathan, A.-S. K., Dai, T. T., and Hong, C. S., "A Key Management Scheme with Encoding and Improved Security for Wireless Sensor Networks," LNCS 4317, Springer-Verlag 2006, pp. 102–115.

[64] Jolly, G., Kuşçu, M. C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks," Proc. of the Eighth IEEE International Symposium on Computers and Communication (ISCC 2003), pp. 335–340.

[65] Huang, D., Mehta, M., Medhi, D., and Harn, L., "Location-aware Key Management Scheme for Wireless Sensor Networks," Proc. of ACM SASN'04, Washington, DC, USA, 2004, pp. 29–42.

[66] Dutertre, B., Cheung, S., and Levy, J. Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust. SDL Technical Report SRI-SDL-04-02, SRI International.

[67] Lee, Y.-H., Phadke, V., Deshmukh, A., and Lee, J. W., "Key Management in Wireless Sensor Networks," ESAS 2004, LNCS 3313, Springer-Verlag, pp. 190–204.

[68] Liu, D., Ning, P., and Li, R., "Establishing Pairwise Keys in Distributed Sensor Networks," ACM Transactions on Information and System Security, Vol. 8, No. 1, 2005, pp. 41–77.

[69] An, F., Cheng, X., Rivera, J. M., Li, J., and Cheng, Z., "PKM: A Pairwise Key Management Scheme for Wireless Sensor networks," ICCNMC 2005, LNCS 3619, Springer-Verlag, pp. 992–1001.

[70] Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., and Khalili, A., "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," ACM Transactions on Information and System Security, Vol. 8, No. 2, 2005, pp. 228–258.

[71] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," IEEE Transactions on Dependable and Secure Computing, Volume 3, Number 2, 2006, pp. 62–77.

[72] Yang, C., Zhou, J., Zhang, W., and Wong, J., "Pairwise Key Establishment for Large-Scale Sensor Networks: from Identifier-based to Location-based," Proc. of the First International Conference on Scalable Information Systems, Hong Kong, 2006.

[73] Dai, T. T., Pathan, A.-S. K., and Hong, C. S., "A Resource-Optimal Key Pre-distribution Scheme with Improved Security for Wireless Sensor Networks," APNOMS 2006, LNCS 4238, Springer-Verlag, pp. 546–549.

[74] Çamtepe, S. A. and Yener, B., "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," IEEE/ACM Transactions on Networking, Vol.15 No.2, 2007, pp. 346–358.

[75] Chorzempa, M., Park, J.-M., and Eltoweissy, M., "Key Management for Long-Lived Sensor Networks in Hostile Environments," Computer Communications, Vol. 30, 2007, pp. 1964–1979.

[76] Großschädl, J., Szekely, A., and Tillich, S., "The Energy Cost of Cryptographic Key Establishment in Wireless Sensor Networks," Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), pp. 380–382.

[77] Huang, D., Mehta, M., Liefvoort, A.V.D., and Medhi, D., "Modeling Pairwise Key Establishment for Random Key Predistribution in Large-Scale Sensor Networks," IEEE/ACM Transactions on Networking, Vol. 15, No. 5, 2007, pp. 1204–1215.

[78] Huang, D. and Medhi, D., "Secure Pairwise Key Establishment in Large-Scale Sensor Networks: An Area Partitioning and Multigroup Key Predistribution Approach," ACM Transactions on Sensor Networks, Vol. 3, No. 3, Article 16, 2007.

[79] Zhang, W., Tran, M., Zhu, S., and Cao, G., "A Random Perturbation-Based Scheme for Pairwise Key Establishment in Sensor Networks," Proc. of ACM MobiHoc2007, pp. 90–99.

[80] Chan, S.-P., Poovendran, R., and Sun, M.-T., "A Key Management Scheme in Distributed Sensor Networks Using Attacks Probabilities," Proc. of IEEE GLOBECOM 2005, Volume 2.

[81] Chan, H., Perrig, A., and Song, D., "Random Key Predistribution Schemes for Sensor Networks," Proc. of Security and Privacy Symposium 2003, pp. 197–213.

[82] Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., and Galloway, M., "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Communications, Vol. 30, 2007, pp. 2314–2341.

[83] Younis, M. and Akkaya, K., "A Survey on Routing Protocols for Wireless Sensor Networks," Ad Hoc Networks, Vol. 3, 2007, pp. 325–349.

[84] Karl, H. and Willig, A. Protocols and Architectures for Wireless Sensor Networks, Wiley, 2006.

[85] Wang, X., Gu, W., Chellappan, S., Schosek, K., and Xuan, D., "Lifetime Optimization of Sensor Networks Under Physical Attacks," Proc. of 2005 IEEE International Conference on Commmunications (ICC 2005), Volume 5, pp. 3295–3301.

[86] Wang, X., Gu, W., Schosek, K., Chellappan, S., and Xuan, D., "Sensor Network Configuration Under Physical Attacks," ICCNMC 2005, LNCS 3619, Springer-Verlag 2005, pp. 23–32.

[87] Warneke, B. A. and Pister, K. S. J., "MEMS for Distributed Wireless Sensor Networks," Proc. of the 9th IEEE International Conference on Electronics, Circuits and Systems, Volume 1, Dubrovnik, Croatia, 2002, pp. 291–294.

[88] http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/Imote2_Datasheet.pdf

[89] Akyildiz, I. F., Melodia, T., and Chowdhury, K. R., "A Survey on Wireless Multimedia Sensor Networks," Computer Networks, Vol. 51, 2007, pp. 921–260.

[90] Gurses, E. and Akan, O. B., "Multimedia Communication in Wireless Sensor Networks," Annals of Telecommunications, Vol. 60, No. 7-8, 2005, pp. 799–827.

[91] Pathan, A.-S. K., Heo, G. and Hong, C. S., "A Secure Lightweight Approach of Node Membership Verification in Dense HDSN," Proc. of the IEEE Military Communications Conference (IEEE MILCOM 2007), Orlando, Florida, USA.

[92] Gu, L., Jia, D., Vicaire, P., Yan, T., Luo, L., Tirumala, A., Cao, Q., He, T., Stankovic, J. A., Abdelzaher, T., and Krogh, B. H., "Lightweight Detection and Classification for Wireless Sensor Networks in Realistic Environments," Proc. of ACM SenSys 2005, San Diego, California, USA, pp. 205–217.

[93] Dutta, P., Grimmer, M., Arora, A., Bibyk, S., and Culler, D., "Design of a Wireless Sensor Network Platform for Detecting Rare, Random, and Ephemeral Events," Proc. of the 3rd symposium on Information Processing in Sensor Networks (IPSN'05), LA, California, pp. 497–502.

[94] Carman, D.W., Kruss, P.S. and Matt, B.J. Constraints and Approaches for Distributed Sensor Network Security. NAI Labs Technical Report # 00-010, dated 1 September, 2000.

[95] Nowak, R.D., "Distributed EM ALgorithms for Density Estimation and Clustering in Sensor Networks," IEEE Transactions on Signal Processing, V. 51, N. 8, 2003, pp. 2245-2253.

[96] Halgamuge, M.N., Guru, S.M. and Jennings, A., "Energy Efficient Cluster Formation in Wireless Sensor Networks," Proceedings of the 10th International Conference on Telecommunications, Volume 2, 2003, pp. 1571-1576.

[97] Lee, S., Yoo, J. and Chung, T., "Distance-based Energy Efficient Clustering for Wireless Sensor Networks," Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, 2004, pp. 567-568.

[98] Younis, O. and Fahmy, S., "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach," IEEE Transactions on Mobile Computing, 3(4), 2004, pp. 366-379.

[99] Ye, M., Li, C., Chen, G. and Wu, J., "EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks," Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference, 2005, pp. 535-540.

[100] Liu, J.-S. and Lin, C.-H.R., "Power-Efficiency Clustering Method with Power-Limit Constraint for Sensor Networks," Proceedings of the 2003 IEEE International Performance, Computing, and Communications Conference, 2003, pp. 129-136.

[101] Gupta, G. and Younis, M., "Load-Balanced Clustering of Wireless Sensor Networks," Proceedings of IEEE International Conference on Communications (ICC'03), Volume 3, 2003, pp. 1848-1852.

[102] Tzevelekas, L., Ziviani, A., Amorim, M.D.D., Todorova, P. and Stavrakakis, I., "Towards Potential-Based Clustering for Wireless Sensor Networks," Proceedings of the 2005 ACM conference on Emerging network experiment and technology, Toulouse, France, 2005, pp. 292-293.

[103] Wokoma, I., Sacks, L. and Marshall, I., "Clustering in Sensor Networks using Quorum Sensing," in the London Communications Symposium, University College London, 2003.

[104] Banerjee, S. and Khuller, S., "A Clustering Scheme for Hierarchical Control in Multi-hop Wireless Networks," Proceedings of IEEE INFOCOM 2001, Volume 2, 2001, pp. 1028-1037.

[105] Mathew, R., Younis, M. and Elsharkawy, S.M., "Energy-efficient bootstrapping for wireless sensor networks," Innovations Syst. Softw. Eng., Vol. 1, No. 2, Springer London, 2005, pp. 205-220.

[106] Prasad, N. R. and Alam, M., "Security Framework for Wireless Sensor Networks," Wireless Personal Communications, V. 37, No. 3-4, Springer Netherlands 2006, pp. 455-469.

[107] Bohge, M. and Trappe, W., "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proceedings of ACM WiSE'03, San Diego, CA, USA, 2003, pp.79-87.

[108] Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proc. of 33rd Annual Hawaii International Conference on System Sciences (HICSS 2000), pp. 3005-3014.

[109] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., and Culler, D. E., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, 8, 2002, pp. 521-534.

[110] Ferreira, A.C., Vilaça, M.A., Oliveira, L.B., Habib, E., Wong, H.C. and Loureiro, A.A., "On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks," ICN 2005, LNCS 3420, Springer-Verlag 2005, pp. 449-458.

[111] Oliveira, L.B., Wong, H.C., Bern, M., Dahab, R. and Loureiro, A.A.F., "SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks," Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications, 2006, pp.145-154.

[112] Wood, A.D., Stankovic, J.A. and Son, S.H., "JAM: A Jammed-Area Mapping Service for Sensor Networks," in the 24th IEEE Real-Time Systems Symposium (RTSS'03), 2003, pp. 286-297.

[113] Clark, B.N., Colbourn, C.J. and Johnson, D. S. Unit Disk Graphs. Discrete Mathematics, 86, pp. 165-177.

[114] Garey, M.L. and Johnson, D.S. Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman, San Francisco, 1979.

[115] Pathan, A.-S.K. and Hong, C.S., "A Key-Predistribution-Based Weakly Connected Dominating Set for Secure Clustering in DSN," HPCC 2006, LNCS 4208, Springer-Verlag 2006, pp. 270-279.

[116] Das, B. and Bharghavan, V., "Routing in Ad-Hoc Networks Using Minimum Connected Dominating Sets," Proceedings of the IEEE International Conference on Communications (ICC 1997), pp. 376-380.

[117] Erdös and Rényi, On Random Graphs. Publicationes Mathematicae, Vol. 6, 1959, pp. 290–297.

[118] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Net-works: A Survey," Computer Networks, Vol. 38, 2002, pp. 393-422.

[119] Dai, S, Jing, X, and Li, L., "Research and analysis on routing protocols for wireless sensor networks," Proceedings of the International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[120] Pathan, A.-S. K. and Hong, C. S., "A Secure Energy-Efficient Routing Protocol for WSN," ISPA 2007, LNCS 4742, Springer-Verlag 2007, pp. 407-418.

[121] Çam, H., Özdemir, S., Muthuavinashiappan, D., and Nair, P., "Energy Efficient Security Protocol for Wireless Sensor Networks," Proceedings of IEEE 58th Vehicular Technology Conference 2003, VTC'03-Fall, Volume 5, 6-9 October 2003, pp. 2981 – 2984.

[122] Çam, H., Özdemir, S., Nair, P., Muthuavinashiappan, D., and Sanli, H. O., "Energy-efficient Secure Pattern based Data Aggregation for Wireless Sensor Networks," Computer Communications, Volume 29, Issue 4, 2006, pp. 446-455.

[123] Zhu, S., Setia, S., Jajodia, S., and Ning, P., "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," In Proceedings of S&P, 2004, pp. 259-271.

[124] Lee, H. Y. and Cho, T. H., "Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks," LNCS 4317, Springer-Verlag 2006, pp. 116-127.

[125] Azzedine, B., Xiuzhen, C., and Joseph, L., "Energy-aware Data-centric Routing in Microsensor Networks," In Proceedings of the 8th MSWiM'03, San Diego, 2003, 42-49

[126] Hyunh, T. T. and Hong, C. S., "An Energy*Delay Efficient Multi-Hop Routing Scheme for Wireless Sensor Networks," IEICE Transactions on Information and Systems, Vol.E89-D No.5, May 2006, pp. 1654-1661.

[127] Yin, C., Huang, S., Su, P, and Gao, C., "Secure Routing for Large-scale Wireless Sensor Networks," In Proceedings of IEEE ICCT 2003, Volume 2, 9-11 April 2003, pp. 1282 – 1286.

[128] Hass, Z.J., "Design Methodologies for Adaptive and Multimedia Networks," IEEE Communications Magazine, vol. 39, no.11, November 2001, pp. 106-107.

[129] Heinzelman, W. B., Chandrakasan, A. P., and Balakrishnan, H., "An Application-specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions in Wireless Communications, Vol. 1, No. 4, October 2002, pp. 660–670.

[130] Lamport, L. Constructing digital signatures from one-way function. Technical report SRI-CSL-98, SRI International, October 1979.

[131] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/

[132] Coppersmith D. and Jakobsson, M., "Almost Optimal Hash Sequence Traversal," In 6th International Financial Cryptography 2002, Bermuda , March 2002.

[133] Jakobsson, M., "Fractal Hash Sequence Representation and Traversal," In 2002 IEEE International Symposium on Information Theory, Switzerland, July 2002.

[134] Sella, Y., "On the Computation-storage Trade-offs of Hash Chain Traversal," In the 7th International Financial Cryptography Conference, Guadeloupe, January 2003.

[135] Ee, C. T. and Bajcsy, R., "Congestion Control and Fairness for Many-to-One Routing in Sensor Networks," In Proceedings of ACM SenSys'04, 2004, pp. 148-161.

[136] Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M., "Authenticated Routing for Ad Hoc Networks," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 3, MARCH 2005, pp. 598-610.

[137] Hu, Y.-C., Perrig, A., and Johnson, D. B., "Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks," Wireless Networks 11, 2005, pp. 21–38.

[138] Patwardhan, A., Parker, J., Joshi, A., Karygiannis, A., and Iorga, M., "Secure Routing and Intrusion Detection in Adhoc Networks," 3rd IEEE

International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 2005