Documents

Sharmin, A., Motakabber, S.M.A., Hashim, A.H.A.

Trust-based Enhanced ACO Algorithm for Secure Routing in IoT

(2024) *Indonesian Journal of Electrical Engineering and Informatics*, 12 (2), pp. 344-359.

DOI: 10.52549/ijeei.v12i2.5118

Department of Electrical and Computer Engineering, International Islamic University Malaysia, Malaysia

Abstract
The Internet of Things (IoT) is an expanding paradigm of object connectivity using a range of resource types and architectures to deliver ubiquitous and requested services. There are security issues associated with the proliferation of IoT-connected devices, allowing IoT applications to evolve. In order to provide an energy-efficient and secure routing method for sensors deployed within a dynamic IoT network, this paper presents a trust-aware enhanced ant colony optimization (ACO)-based routing algorithm, incorporating a lightweight trust evaluation model. As it is challenging to implement security in resource-constrained IoT networks, the presented model adopted bio-inspired approaches, offering an improved version of ACO towards secure data transmission cost-effectively while taking into consideration residual energy and the trust score of the sensor to be optimized. The trust evaluation system has been enhanced in the development of the proposed routing algorithm and the node trust value is evaluated, sensor node misbehavior is identified, and energy conservation is maximized. The performance evaluation is demonstrated utilizing MATLAB. In comparison to the standard bio-inspired algorithms and existing secure routing protocols, the proposed system reduces average energy consumption by nearly 50% regardless of the increase in the number of nodes and end-to-end delay of 40%, while finding the secure and optimal path in unison is designed to ensure trust in the IoT environment.

Author Keywords
Ant Colony Optimization; Energy efficiency; Internet of Things; Secure Routing; Sensors; Trust Evaluation

References

- Pereira, F., Correia, R., Pinho, P., Lopes, S. I., Carvalho, N.B.
  Challenges in resource-constrained IoT devices: Energy and communication as critical success factors for future IoT deployment
  (2020) *Sensors (Basel)*, 20, p. 6420.

- Granjal, J., Monteiro, E., Sa Silva, J.
  Security for the internet of things: A survey of existing protocols and open research issues
  (2015) *IEEE Communications Surveys and Tutorials*, 17 (3), pp. 1294-1312.

- Ganeriwal, S., Srivastava, M. B.
  Reputation-based framework for high integrity sensor networks
  (2004) *SASN'04: Proceedings of the 2nd ACM workshop on security of Ad hoc and sensor networks*, pp. 66-77.
  New York: ACM

- Hamrioui, S., Lorenz, P.
  Bio inspired routing algorithm and efficient communications within IoT
  (2017) *IEEE Network*, 31 (5), pp. 74-79.

- Xia, H., Jia, Z., Sha, E. H.-M.
  Research of trust model based on fuzzy theory in mobile ad hoc networks
  (2014) *IET Inf. Secur*, 8 (2), pp. 88-103.
  March

- Gladkov, A., Shiriaev, E., Tchernykh, A., Deryabin, M., Babenko, M., Nesmachnow, S.
  DT-RRNS: Routing protocol design for secure and reliable distributed smart sensors communication systems
  (2023) *Sensors (Basel)*, 23 (7), p. 3738.

- Kenji, I., Matsunaga, T., Toyoda, K., Sasase, I.
  Secure parent node selection scheme in route construction to exclude attacking nodes

from RPL network
(2015) *IEICE Communications Express*, pp. 299-303.

- Solapure, S. S., Kenchannavar, H. H.
Design and analysis of RPL objective functions using variant routing metrics for IoT applications
(2020) *Wireless Networks*, 26, pp. 4637-4656.

- Glissa, G., Rachedi, A., Meddeb, A.
A Secure Routing Protocol Based on RPL for Internet of Things
(2016) *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-7.

- Liu, X., Yu, J., Yu, K., Wang, G., Feng, X.
Trust secure data aggregation in WSN-based IIoT with single mobile sink
(2022) *Ad Hoc Netw*, 136, p. 102956.

- Stephen, R., Arockiam, L.
E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things
(2018) *Journal of Physics: Conference Series*, 1142 (1), p. 012009.

- Yamamoto, R., Nishibu, S., Yamazaki, T., Okamura, Y., Tanaka, Y.
ACO-inspired energy-aware routing algorithm for wireless sensor networks
(2019) *Journal of Telecommunications and Information Technology*,

- Sharmin, A., Anwar, F., Motakabber, S.M.A., Hashim, A.H.A.
Secure ACO-Based Wireless Sensor Network Routing Algorithm for IoT
Proceedings of the 8th International Conference on Computer and Communication Engineering, ICCCE 2021, 2021, pp. 190-195.

- Sharmin, A., Anwar, F., Motakabber, S.M.A., Hashim, A.H.A.
A Trust Aware Secure Ant Colony Optimization Based Routing Algorithm for Internet of Things
2023 IEEE 9th International Conference on Computer and Communication Engineering, ICCCE 2023, 2023, pp. 58-63.

- Heinzelman, W. B., Chandrakasan, A. P., Balakrishnan, H.
An application-specific protocol architecture for wireless microsensor networks
(2002) *IEEE Transactions on Wireless Communications*, 1 (4), pp. 660-670.

- Fang, W., Zhang, X., Shi, Z., Sun, Y., Shan, L.
Binomial-based trust management system in wireless sensor networks
(2017) *Chin. J. Sens. Actuators*, 28 (5), pp. 703-708.

- Vasseur, J., Kim, M., Pister, K., Dejean, N., Barthel, D.
Routing metrics used for path calculation in low power and lossy networks
(2011) *Draft-Ietf-Roll-Routing-Metrics*,

- Winter T., Winter T., Thubert P., Thubert P.
RPL: IPv6 Routing Protocol for Low power and Lossy Networks
(2010) *IETF Internet-Draft*,
Ed. and, Ed

- Muzammal, S. M., Murugesan, R. K., Jhanjhi, N. Z., Hossain, M. S., Yassine, A.
Trust and mobility-based protocol for secure routing in Internet of Things
(2022) *Sensors (Basel)*,

- Tanveer, M., Abbas, G., Abbas, Z. H., Waqas, M., Muhammad, F., Kim, S.
S6AE: Securing 6LoWPAN using authenticated encryption scheme
(2020) *Sensors (Basel)*,

- Nichols, K., Jacobson, V., King, R.
Defined-Trust Transport (DeftT) Protocol for Limited Domains,
(accessed on 5 March 2023)

- Granjal, J., Silva, J. M., Lourenço, N.
Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection
(2018) *Sensors (Basel)*,

- Shafer, G.
(1976) *A mathematical theory of evidence*, 42.
Princeton university press

- Dodds, D. R.
Fuzziness in knowledge-based robotics systems
(1988) *Fuzzy sets and systems*, 26 (2), pp. 179-193.

- Josang, A., Ismail, R.
The beta reputation system
(2002) *Proceedings of the 15th bled electronic commerce conference*, 5, pp. 2502-2511.
June

Correspondence Address
Sharmin A.; Department of Electrical and Computer Engineering, Malaysia; email: afsahsharmin@gmail.com

Publisher: Institute of Advanced Engineering and Science

ISSN: 20893272
Language of Original Document: English
Abbreviated Source Title: Indones. J. Electr. Eng. Informatics
2-s2.0-85199310730
Document Type: Article
Publication Stage: Final
Source: Scopus