International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 08th Dec 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-12

DOI: 10.48047/IJIEMR/V10/I12/03

Title A Survey on Efficient Secure Routing in Industrial Network for Improved QoS

Volume 10, Issue 12, Pages: 13-21

Paper Authors

Babu N, Dr.Tamilarasi Suresh

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Survey on Efficient Secure Routing in Industrial Network for Improved QoS

Babu N[1], Dr.Tamilarasi Suresh[2]

Research Scholar, St. Peter's Institute of Higher Education and Research,
babuskpt@gmail.com,
Professor, Department of IT,St. Peter's Institute of Higher Education and Research,
tamilarasisu@gmail.com

Abstract:
The industrial units adapt different networks for the management of their units, processes and resources. The industrial sector uses different networks for their smooth functioning which would require accessing various network services by their users, employees and customers. However, the industrial networks arenot exemptions from network threats. Number of threats exist which challenge the functioning of industrial network like DDoS (Distributed Denial of Service), black hole, eavesdrop attack and so on. Most attacks focus towards degrading the QoS performance of industrial network. To handle this, different approaches are available in literature which works based on several features like traffic, hop count, payload, service frequency, retransmission frequency, node behaviors, and location of nodes and so on. Similarly, most threats occur over the routing procedure. Towards maximizing the QoS of industrial network, it is necessary to analyze various routing protocols and their way of handling different threats. This article analyzes various routing protocols and threats towards QoS of Industrial networks.

Keywords: Industrial Networks, Network Services, Network Threat, Attacks, Secure Routing, QoS.

1. Introduction:

The growth of information technology supports organizations in several ways.Various industries use their own network to provide services to their employees to perform different tasks. For example, by deploying their own network, the units which are distributed geographically can communicate with each other and access different resources independent of their location. This enables their customers and employees to access various resources through number of network services which are dedicated to them. The industrial networks maintain its own network to communicate within its network as well as with the external world.

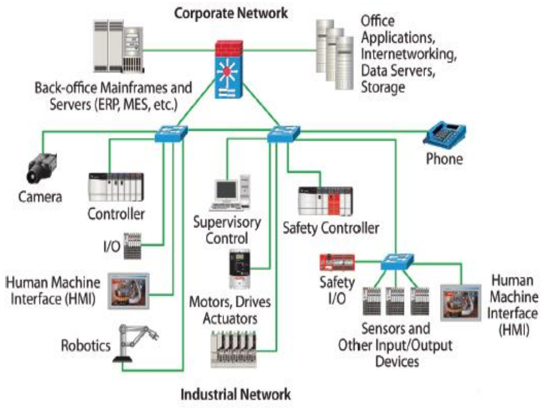
Corporate Network
Office Applications, Internetworking, Data Servers, Storage
Back-office Mainframes and Servers (ERP, MES, etc.)
Phone
Camera
Controller
I/O
Supervisory Control
Safety Controller
Human Machine Interface (HMI)
Motors, Drives Actuators
Safety I/O
Human Machine Interface (HMI)
Robotics
Sensors and Other Input/Output Devices
Industrial Network

Figure 1: Industrial Network Architecture

The topology of industrial network is presented in Figure 1, which consists of various components like controller, supervisory controller, safety controller, human machine interface, sensors, camera, robotics and back office servers and other office applications.

1.2 Security Threats on Industrial Networks:

There are number of security threats presented in industrial networks. Among them there are few risks which are more important and listed below:

- **Network Configuration:**

  The network configuration plays vital role in achieving higher security. When the network is not configured well, then the intruder or attacker can generate attacks successfully. For example, if a device is exposed to external world without being securely configured, then the intruder can breach the security wall easily.

- **Log Tracing:**

Presence of logging system is essential to monitor the network. If there is no logging system, then monitoring and controlling the system would fail.

- **Lack of Control:**

Presence of asset management in a centralized and automated way is much important. So, the assets must be monitored and controlled with centralized control which challenges the adversary.

- **Employee Ignorance:**

Phishing attacks, social engineering, and risky browsing behaviors all threaten to punch a hole that can be exploited by attackers to compromise the IT, OT or both networks via lateral movement. Security training, network segmentation, and multifactor authentication can together prevent breaches caused by employee's lack of awareness, policy violations, or human error.

- **Insider Attacks:**

Insider attack is the most challenging issue to be handled in the industrial network. So, monitoring and verifying the trust of the user is more important.

2. Literature Survey:

The methods of threat detection and secure routing have been classified in to several cases in this section. Intrusion detection has been applied in several applications and an important challenge is building the secure intrusion detection system in network providing security to the nodes and route paths in the network. The attacks in network can threaten the security issues which have been identified in the intrusion detection system engine, later it is prevented by intrusion prevention engine in the network. And henceforth new technique to implement the security goals and prevent attacks is implemented by introducing the Secure-Intrusion Detection System (S-IDS) in the network [2]. Similarly, there are many secure routing schemes different threats and a short correlation of different protocols accessible for anchored routing in MANET along with basic characteristics and challenges of MANET are explained.[27] In [29], a contemporary review of communication architectures and topographies for MANET-connected Internet-of-Things (IoT) systems is presented.

Various approaches of secure routing scheme is analyzed such as SAR, SEAD, and ARAN etc. have been analyzed on the basis of their underlying security mechanism, scalability, overhead etc [31]. Similarly, in [33], a set of multi tier energy systems are analyzed for their performance in intrusion detection. In [34], the author discusses the requirement of intrusion detection systems in the network. In [45], the author discusses the requirement of secure routing scheme where data aggregation is performed. The impact of energy of nodes in routing has been discussed in detail in [46]. According to this, the methods of secure routing are classified as follows:

2.1 Trust Based Secure Routing:

A trust based hybrid secure routing scheme (S-DSR) is presented in [24], which uses the trust value of nodes collected from neighbor nodes in establishing secure route for communication. A trust sensing-based secure routing mechanism (TSSRM) with the lightweight characteristics and the ability to resist many common attacks simultaneously is proposed in [50]. A Q learning based efficient secure routing (ESRQ) is presented in [52], which computes the trust according to the behavior of the nodes. A trust based secure energy efficient routing (TSER) is presented in [54], which select the route according to hop count, energy. The nodes are authenticated based on key exchange and messages.

A trust and packet load balancing based opportunistic routing (TPBOR) scheme is presented in [44], which measure the trust of road according to energy and distribute the traffic in different routes presented in [26], which computes the reputation of nodes and maintained in legitimacy value table.

2.2 Cryptography Based Secure Routing:

Secure and practical access control mechanism for WSN with node privacy [9], a provable and practical access control scheme based on Elliptical Curve Cryptography (ECC) has been presented. The proposed access control scheme supports node privacy while addressing all other major functional and security requirements. The formal validation of the proposed scheme has been carried out using automated validation of internet security protocols and applications (AVISPA) and Scyther tools.

Secure Routing in Cluster-Based Wireless Sensor Networks [47], proposes a new secure protocol based on the well-known LEACH routing protocol named Hybrid Cryptography-Based Scheme for secure data communication in cluster-based WSN (HCBS). As a multi-constrained criteria approach, HCBS is built on a combination of the cryptography technique based on Elliptic Curves to exchange keys that uses symmetric keys for data encryption and MAC operations.

2.3 Energy Based Secure Routing:

Joint Energy-Saving Scheduling and Secure Routing for Critical Event Reporting in Wireless Sensor Networks [16], combined with the level-by-level sleeping scheduling method, the energy-saving and secure uplink transmission can be guaranteed. In the downlink, an energy-first multi-point relays set selection mechanism (EFMSS) is designed to choose the backbone nodes to broadcast messages, and the backbone nodes are woken up by the same level-by-level sleeping scheduling method as the uplink transmission. With the two-step procedure, the critical events are appropriately dealt with and the responses are broadcasted to the whole network.

An Energy Efficient Secure Routing (EESR) using Elliptic Curve Cryptography for Wireless Sensor Networks [48], proposes inter and intra cluster head selection method which consumes less energy and increase the network lifetime.

Energy Efficient & Secured Data Routing Through Aggregation Node in WSN [51], makes use of the Iterative Filtering (IF) algorithm, which additionally gives trust evaluation to the numerous sources from where the information is aggregated.

Enhanced Energy Efficient Secure Routing Protocol For Mobile Ad-Hoc Network [3], proposes the Enhanced Energy Efficient-Secure Routing (EEE-SR) protocol as a novel security algorithm to access secure data in hostile environment

SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks [4], In first phase of the research, network and routing assumptions are made to initialize the effective packet transmission. In second phase, stability metric is determined for the cluster to maximize the energy efficiency

ECIGC-MWSN: Energy capable information gathering in clustered secured CH based routing in MWSN [10], an energy capable information gathering plan for clustered nano sensor arrangement for mobile wireless nano sensor network is introduced.

Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network [19], makes use of an artificial intelligence-based heuristic analysis to accomplish a reliable, and intellectual learning scheme. Secondly, it protects the transmissions against adversary groups to attain security with the least complexity.

2.4 Tree Based Secure Routing:

A Secure Hybrid Routing Protocol for Mobile Ad-Hoc Networks [21], a secure hybrid routing protocol that uses proactive and reactive techniques for establishment of routes, where MANET topology and MST (minimum spanning tree) are proactively developed and the routes for data transmission are established reactively using MST obtained in proactive phase.

Cluster based Intrusion Detection System for Mobile Ad-hoc Network [36], proposes CBIDP (cluster based Intrusion detection planning) an effective clustering algorithm which is ahead of the existing routing protocol. Decision Tree based AIS strategy for Intrusion Detection in MANET [37], discuss that Intrusion Detection strategy used in wired networks are unbefitting for wireless networks due to reasons not limited to resource constraints of participating nodes and nature of communication. Secured algorithm for routing the military field data using Dynamic Sink: WSN [42], propose LISA algorithm along with Steiner Minimal Tree algorithm to route data in a Secured manner. LISA algorithm provides both confidentiality and integrity to data.

2.5 Traffic Based Secure Routing:

Secure and load balanced routing model for wireless sensor networks [5], proposes a secure and load balanced routing (SLBR) scheme for heterogeneous clustered based WSNs. SLBR presents a better trust-based security metric that overcomes the problem when sensors keep oscillating from good to bad state and vice versa, and also SLBR balances load among CH. Thus, aids in achieving better security, packet transmission, and energy efficiency performance.

DSOR: A Traffic-Differentiated Secure opportunistic Routing with Game Theoretic Approach in MANETs [23], propose a traffic-differentiated secure opportunistic routing from a game theoretic perspective, DSOR. In the proposed scheme, we use a novel method to calculate trust value, considering node's forwarding capability and the status of different types of flows. According to the resource status of the network, we propose a service price and resource price for the auction model, which is used to select optimal candidate forwarding sets. At the same time, the optimal bid price has been proved and a novel flow priority decision for transmission is presented, which is based on waiting time and requested time.

2.6 Location Based Secure Routing:

An efficient biometric based authenticated geographic opportunistic routing for IoT applications using secure wireless sensor network [6], propose a new scheme of security algorithm for the wireless sensor networks. Our method, Biometric based-Authenticated Geographic Opportunistic Routing (BAGOR) algorithm depends on the user biometrics to shield the violation of DoS attacks, in order to meet out the validness requirements and reliability in the network.

2.7 Behavior based Approach:

Novel Intrusion Detection and Prevention for Mobile Ad Hoc Networks: A Single- and Multiattack Case Study [39], present novel techniques to counter a set of active attacks, such as denial-of-service (DoS), probe, vampire, and user-to-root (U2R) attacks, in a mobile ad hoc network (MANET) environment for a single- and multiattack scenario. Attacks are detected using a profile (behavior) analysis for single attacks and a distributed trust for multiattacks.

List of Routing methods, Advantages and Disadvantages from Existing Research papers

- **Paper 1:** (V. S. Bhargavi, et. al 2016)

Routing Method Used: Trust Sensing Based Secure Routing (TSSRM). Measures Trust value based on the information collected from neighbor nodes.

Advantages: The selection of route is performed based on the trust value measured which would improve security performance.

Disadvantages: Presence of malicious node would provide fake information which would affect the routing performance. Also introduces higher network overhead at the trust collection.

- **Paper 2:** (HIlmiLazrag, et. al 2016)

Routing Method Used: Q learning based efficient secure routing (ESRQ). Measures the trust value according to the behavior of nodes

Advantages: Introduces higher security performance.

Disadvantages: The efficiency of routing is depending on the logs available about the behavior of nodes.

- **Paper 3:** (G. M. Navami Patil, 2017)

Routing Method Used: A trust based secure energy efficient routing (TSER).

Performs secure routing based on hop count and energy.

Advantages: Introduces higher security performance by measuring trust according to hop count and energy.

Disadvantages: The efficiency of the protocol is depending on the information available, and introduces higher overhead in the data collection.

- **Paper 4:** (M. Mishra, G. S. Gupta and X. Gui, 2017)

Routing Method Used: A trust and packet load balancing based opportunistic routing (TPBOR). Measures the trust according to the energy.

Advantages: Performance of route selection is higher.

Disadvantages: Introduces higher energy depletion at all the routes by distributing the traffic in all the routes. This affects the lifetime of entire network.

- **Paper 5:** (R. Shukla, et. al 2017)

Routing Method Used: Energy Efficient Secure Routing (EESR) using Elliptic Curve Cryptography. Uses inter intra cluster selection method in routing. Also. ECC has been used in security development.

Advantages: Improves security performance.

Disadvantages: Introduces poor throughput performance.

- **Paper 6:** (D. Qin, et. al 2017)

Routing Method Used: Trust and energy aware secure routing protocol (TESRP). Performs route selection based on the trust which is computed using the sequence number

Advantages: Improves security performance in data transmission

Disadvantages: Suffer with poor throughput performance.

- **Paper 7:** (C. Deepa and B. Latha, 2018)

Routing Method Used: Hybrid Cryptography-Based Scheme (HCBS). Uses ECC in data encryption towards access restriction. Also, secure routing is performed using LEACH.

Advantages: Introduces higher security performance.

Disadvantages: Time complexity is higher.

- **Paper 8:** (S. Gopalakrishnan and A. Rajesh, 2019)

Routing Method Used:CBIDP (cluster-based Intrusion detection planning). Performs intrusion detection with collaborative nature

Advantages: Reduces memory overhead.

Disadvantages: Suffer with higher time complexity.

- **Paper 9:** (X. Zhong, et. al 2019)

Routing Method Used:DSOR: A Traffic-Differentiated Secure opportunistic Routing. Uses game theory in identifying a secure routing. Computes trust value based on the capability of nodes in forwarding the packets.

Advantages: Improves throughput performance

Disadvantages: Suffer with moderate secure routing performance.

- **Paper 10**: (UmmerIqbal, 2020)

Routing Method Used: automated validation of internet security protocols and applications (AVISPA). Uses Elliptic Curve Cryptography in access control and secure routing.

Advantages: Improves secure routing performance.

Disadvantages: Introduces higher time complexity as the time complexity of ECC is higher which is not suitable for service orient environment.

- **Paper 11:** (W. Feng et al, 2020)

Routing Method Used: Energy-first multi-point relays set selection mechanism (EFMSS). Performs route selection according to energy. Performs scheduling at each level of the network

Advantages: Introduces higher throughput performance.

Disadvantages: Suffers with poor security performance

- **Paper 12:** (K. Haseeb, et. al 2020)

Routing Method Used: Secure and Energy-Aware Heuristic Routing Protocol. Uses artificial intelligence-based heuristic analysis for reliable routing.

Advantages: Improves secure routing performance

Disadvantages: Suffer with poor throughput performance

- **Paper 13:** (Nippun Kamboj et. al 2020)

Routing Method Used: Enhanced Energy Efficient Secure-AODV (EEES-AODV). Uses energy as the key metric in route selection.

Advantages: Improves security performance.

Disadvantages: The throughput performances gets reduced at time goes

- **Paper 14:** (K. Biswas and M. Dasgupta, 2020)

Routing Method Used: secure hybrid routing protocol. Uses minimum span tree in organizing the network structure and performs routing. Uses proactive information in route selection.

Advantages: Introduces moderate security performance

Disadvantages: Suffer with higher time complexity.

- **Paper 15:** (GousiaThahniyath, 2020)

Routing Method Used: secure and load balanced routing (SLBR). Measures trust value based on different parameters

Advantages: Introduces higher security performance

Disadvantages: Suffer with poor throughput performance.

- **Paper 16:** (RajendraPrasad P, 2021)

Routing Method Used: Enhanced Energy Efficient-Secure Routing (EEE-SR). Uses energy and trust policies in the route selection and to identify a secure route.

Advantages: Improves security performance

Disadvantages: The performance of approach is depending on the entries in the policies. Not suitable for undefined clients.

- **Paper 17:**(S.Gopinath, 2021)

Routing Method Used:SCEER: Secure cluster based efficient energy routing.

Uses stability metric in identifying a stable route and stability of the cluster. Based on energy and stability the route selection is performed.

Advantages: Improves the security performance.

Disadvantages: The throughput performance is not up to expected level

- **Paper 18:**(S.Menaga,et. al 2021)

Routing Method Used: Biometric Based-Authenticated Geographic Opportunistic Routing (BAGOR) use biometric in identifying the Dos attacks.

Advantages: Improves security as well as throughput performance

Disadvantages: Suffer with unknown handling attacks

- **Paper 19:**(M. Rathee, et. al 2021)

Routing Method Used:ant colony optimization based QoS aware energy balancing secure routing (QEBSR). Uses ant colony in efficient routing.

Advantages: Improves security performance.

Disadvantages: Introduces higher overhead.

3. Summary:

The problems of secure routing in industrial networks are well discussed. The methods available towards secure routing in industrial network are analyzed for their performance. Each method has been analyzed for the factor and feature used. Advantages and disadvantages are analyzed.. The methods are classified under different sections according to their nature and type. A detailed comparative study has been presented in the paper.

REFERENCES:

1. Hwanseok Yang, A Study on Improving Secure Routing Performance Using Trust Model in MANET, HINDAWI (MIS), Volume 2020, 2020.
2. RajendraPrasad, SECURE INTRUSION DETECTION SYSTEM ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORK, SCIENCE DIRECT (GTP), 2021.
3. RajendraPrasad P, ENHANCED ENERGY EFFICIENT SECURE ROUTING
4. CH based routing in MWSN, SCIENCE DIRECT (MP), Volume 43, PP 3457-462, 2021.
5. A. K. Biswas and M. Dasgupta, "A Secure Hybrid Routing Protocol for Mobile Ad-Hoc Networks (MANETs)," IEEE (ICCCNT), 2020, pp. 1-7.
6. J. Tu, D. Tian and Y. Wang, "An Active-Routing Authentication Scheme in MANET," IEEE, Volume. 9, pp. 34276-34286, 2021.
7. S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," IEEE (iEECON), 2020, pp. 1-4.
8. G. Vaseer, "Multi-Attack Detection using Forensics and Neural Network based Prevention for Secure MANETs," IEEE (ICCCNT), 2020, pp. 1-6.
9. X. Zhong, R. Lu, L. Li, X. Wang and Y. Zheng, "DSOR: A Traffic-Differentiated Secure opportunistic Routing with Game Theoretic Approach in MANETs," IEEE (ISCC), 2019, pp. 1-6.
10. W. Feng et al., "Joint Energy-Saving Scheduling and Secure Routing for Critical Event Reporting in Wireless Sensor Networks," IEEE, Volume. 8, pp. 53281-53292, 2020.
11. M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," IEEE (TEM), Volume. 68, Number. 1, pp. 170-182, 2021.
12. K. Haseeb, N. Islam, A. Almogren and I. Ud Din, "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things," IEEE, Volume. 7, pp. 185496-185505, 2019.
13. K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba and U. Tariq, "Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network," IEEE, Volume. 8, pp. 163962-163974, 2020,
14. Nippun Kamboj, Dalip,Dr. Munishwar Rai, An Enhanced Energy Efficient Secure Routing Protocol for MANET, IJAST, Volume 29, Number 5, 2020.
15. K. Biswas and M. Dasgupta, "A Secure Hybrid Routing Protocol for Mobile Ad-Hoc Networks (MANETs)," IEEE (ICCCNT), 2020, pp. 1-7.
16. S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," IEEE (iEECON), 2020, pp. 1-4.
17. X. Zhong, R. Lu, L. Li, X. Wang and Y. Zheng, "DSOR: A Traffic-Differentiated Secure opportunistic Routing with Game Theoretic Approach in MANETs," IEEE (ISCC), 2019, pp. 1-6.
18. V. S. Bhargavi, M. Seetha and S. Viswanadharaju, "A trust based secure routing scheme for MANETS," IEEE (Confluence), 2016, pp. 565-570.
19. S. Yadav, M. C. Trivedi, V. K. Singh and M. L. Kolhe, "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme," IEEE (UPCON), 2017, pp. 1-4.
20. S. Sharma, "A secure reputation based architecture for MANET routing," IEEE (ICECS), 2017, pp. 106-110.
21. N. Yadav and U. Chug, "Secure Routing in MANET:A Review," IEEE (COMITCon), 2019, pp. 375-379.
22. S. S. Kumar and M. Karthick, "An Secured Data Transmission in Manet Networks with Optimizing Link State Routing Protocol Using ACO-CBRP Protocols," IEEE (ICSNS), 2018, pp. 1-8.
23. J. Karlsson, L. S. Dooley and G. Pulkkis, "Secure Routing for MANET Connected

Internet of Things Systems," IEEE (FiCloud), 2018, pp. 114-119.
24. A. K. Biswas and M. Dasgupta, "A Secure Hybrid Routing Protocol for Mobile Ad-Hoc Networks (MANETs)," IEEE (ICCCNT), 2020, pp. 1-7.
25. G. K. Wadhwani, S. K. Khatri and S. K. Muttoo, "Critical Evaluation of Secure Routing Protocols for MANET," IEEE (ICACCCN), 2018, pp. 202-206.
26. S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," IEEE (iEECON), 2020, pp. 1-4.
27. P. P. Rajendra and Shivashankar, "Multitier energy system review on secure intrusion detection system in MANETs," IEEE (RTEICT), 2017, pp. 1722-1726.
28. S. S. Zalte and V. R. Ghorpade, "Intrusion Detection System for MANET," IEEE (I2CT), 2018, pp. 1-4.
29. M. S. Hussain and K. U. R. Khan, "Network-based Anomaly Intrusion Detection System in MANETS," IEEE (ICISC), 2020, pp. 881-886.
30. S. Gopalakrishnan and A. Rajesh, "Cluster based Intrusion Detection System for Mobile Ad-hoc Network," IEEE (ICONSTEM), 2019, pp. 11-15.
31. L. E. Jim and J. Chacko, "Decision Tree based AIS strategy for Intrusion Detection in MANET," IEEE (TENCON), 2019, pp. 1191-1195.
32. K. M. Saifuddin, A. J. B. Ali, A. S. Ahmed, S. S. Alam and A. S. Ahmad, "Watchdog and Pathrater based Intrusion Detection System for MANET," IEEE (iCEEiCT), 2018, pp. 168-173.
33. G. Vaseer, G. Ghai and D. Ghai, "Novel Intrusion Detection and Prevention for Mobile Ad Hoc Networks: A Single- and Multiattack Case Study," IEEE (CEM), volume 8, number 3, pp. 35-39. R. Basomingera and Y. Choi, "Route Cache Based SVM Classifier for Intrusion Detection of Control Packet Attacks in Mobile Ad-Hoc Networks," IEEE (ICOIN), 2019, pp. 31-36.
34. S. Karthick, E. S. Devi and R. V. Nagarajan, "Trust-distrust protocol for the secure routing in wireless sensor networks," IEEE (ICAMMAET), 2017, pp. 1-5.
35. M. Tokala and R. Nallamekala, "Secured algorithm for routing the military field data using Dynamic Sink: WSN," IEEE (ICICCT), 2018, pp. 471-476.
36. B. Patil and R. Kadam, "A novel approach to secure routing protocols in WSN," IEEE (ICISC), 2018, pp. 1094-1097.
37. N. Kumar and Y. Singh, "Trust and packet load balancing based secure opportunistic routing protocol for WSN," IEEE (ISPCC), 2017, pp. 463-467.
38. M. Mishra, G. S. Gupta and X. Gui, "A Review of and a Proposal for Cross-Layer Design for Efficient Routing and Secure Data Aggregation over WSN," IEEE (CINE), 2017, pp. 120-125.
39. B. Bhushan and G. Sahoo, "A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks," IEEE (ICSPC), 2017, pp. 294-299.
40. F. Mezrag, S. Bitam and A. Mellouk, "Secure Routing in Cluster-Based Wireless Sensor Networks," IEEE (GLOBECOM), 2017, pp. 1-6.
41. C. Deepa and B. Latha, "An Energy Efficient Secure Routing (EESR) using Elliptic Curve Cryptography for Wireless Sensor Networks," IEEE (ICICCT), 2018, pp. 1603-1608.
42. R. Shukla, R. Jain and P. D. Vyavahare, "Combating against wormhole attack in trust and energy aware secure routing protocol (TESRP) in wireless sensor network," IEEE (RISE), 2017, pp. 555-561.
43. D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma and Q. Ding, "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network," in IEEE Access, volume 5, pp. 9599-9609, 2017.
44. R. Ashtikar, D. Javale and S. Wakchaure, "Energy Efficient & Secured Data Routing Through Aggregation Node in WSN," IEEE (ICCUBEA), 2017, pp. 1-6.
45. G. Liu, X. Wang, X. Li, J. Hao and Z. Feng, "ESRQ: An Efficient Secure Routing Method in Wireless Sensor Networks Based on Q-Learning," IEEE (TrustCom/BigDataSE), 2018, pp. 149-155.
46. HIlmiLazrag, A Game Theoretic Approach for Optimal and Secure Routing in WSN,

Springer Link (AECIA), Volume 565, 2016, pp 218-228.

47. Komal Saini, A Trust-Based Secure Hybrid Framework for Routing in WSN, Springer Link (RFICT), Volume 707, 2018, pp 585-591.
48. G. M. Navami Patil, Trust Model for Secure Routing and Localizing Malicious Attackers in WSN, Springer Link (CNS), Volume 12, 2017, PP 1-9.
49. M. Kavitha, An efficient city energy management system with secure routing communication using WSN, Springer Link, 2017, PP 1-12.
50. Mohammed zaki Hassan, Lifetime maximization by partitioning approach in wireless sensor networks, Springer Open (WCN), Number 15, 2017.
51. Huiting Xu, Maximizing the lifetime of wireless sensor networks in trains for monitoring long-distance goods transportation, (IJDSN), Volume 13, Issue 5, 2017.
52. Fouad El Hajji, Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks, Springer Link (JCIN), Volume 3, Issue 1, 2018, pp 67–83.