IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 36, No. 2, April, 2022, pp. 289-295
Journal homepage: http://iieta.org/journals/ria

Secure Data Transmission in Wireless Sensor Networks with Secure System for Identification of Trusted Route with Node Behavior Analysis

Minakshi Sahu[1*], Nilambar Sethi[1], Susanta Kumar Das[2]

[1] Department of Computer Science and Engineering, GIET University, Gunupur, Odisha 765022, India
[2] Department of Computer Science, Berhampur University, Bhanja Bihar, Berhampur 760007, India

Corresponding Author Email: meenkashisahu187@gmail.com

https://doi.org/10.18280/ria.360213

Received: 19 December 2021
Accepted: 18 February 2022

Keywords:
routing, trust factor, node behavior, security, prime node, data transmission

ABSTRACT

The Wireless Sensor Network (WSN) is a novel and demanding technology that requires little processing and computational capabilities. In the WSN, security is a serious issue. Because of its wireless nature, it is vulnerable to a wide range of assaults and data packet loss. Secure routing is critical to avoid problems like this. When it comes to data delivery to other nodes, routing is one of the most important WSN method to provide security to the network. Based on the expected trust value, the routing process's trust mechanism prevents/includes nodes in routing. This research examines security objectives for routing the sensor networks and presents an Extreme Trust Factor for Route Identification with Prime Node (ETFRI-PN). The Prime Node (PN) examines each node's behavior throughout the delivery process, as well as computers' ability to detect malicious assaults, and assigns a trust factor to each node involved in data transmission along with Alphanumeric Inimitable Label (AIL) for every node. The proposed model is in contrast to previous models, and the results show that the proposed model outperforms traditional models.

1. INTRODUCTION

A Wireless Sensor Network (WSN) is made up of a large number of interconnected Sensor Nodes (SNs) that can sense physical environment variables including temperature, moisture and sound while also interacting with each other across the wireless medium [1]. Advances in many technologies have resulted in the development of small, low-cost multimedia devices such as video cameras [2] and microphones, which can be easily combined to form a sensor node [3]. Due to the inherent properties that separate WSNs from other wireless networks such as mobile ad hoc networks or cellular networks, routing in these networks is extremely difficult [4].

For starters, a global addressing system for Wi-Fi Sensor Networks that are formed of highly interconnected sensor nodes [5], each of which is able to sense and communicating with other SNs through the wireless medium, is not achievable due to the comparatively large number of sensor nodes. Small, low-cost entertainment gadgets [6] such video microphones and webcams can now be combined to form a sensor node, thanks to advances in technology. WSN routing is highly complex because it differs from other wireless networks such as mobile ad hoc networks [7] or cellular networks.

Nodes in sensor networks frequently demonstrate trust relationships that go beyond those found in ad hoc networks, which is a significant advantage [8]. Nodes in sensor networks that are close to one another are frequently witness to the same or closely related environmental phenomena. In the event that each node responds by sending a packet to the base station, valuable energy and bandwidth are squandered [9]. Sensor networks need in-network processing, aggregation, and duplicate removal in order to prune these redundant messages in order to reduce traffic and conserve electricity [10]. In ad hoc networks, trust relationships between nodes are not often established, as malicious nodes [11] also involve in routing process that degrades the network performance [12]. The available routing protocols in WSN network are shown in Figure 1.

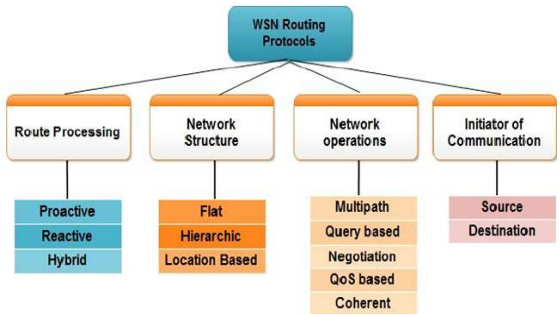

Figure 1. WSN routing protocols

Weak resources and changing topology make WSNs vulnerable to security and computational capabilities concerns [13]. It's now possible to use trust-based methods to handle nodes that behave badly, but there are still a variety of assaults, high energy consumption and congestion [14] in communication between nodes to contend with. On top of all of that, cluster heads determine the safest multiple hop paths, which can actively prevent wormhole attacks.

Routers separate WSN from other networks such as MANET. When using a WSN, routing might be a difficult operation because there are so many sensor nodes installed. As a result of the wireless nature, routing is one of the most important areas to focus on. In order to prevent signal spoofing,

the injection of created messages into the network, and the change of messages during transmission [15], secure routing [16] must be implemented. Error data and system faults may also cause network failure [17]. As a result of attacks and data loss, secure routing is required. In addition, secure routing through a trustworthy node is one technique to avoid the kind of attacks.

To ensure the trustworthiness of a node, trust must be established between nodes [18]. To be considered a trustworthy node [19], a node must be capable of sensing and sending data to the right destination without compromising the integrity or confidentiality of the data [20]. In order to discover the trust node and detect malicious nodes, many different types of techniques are utilized that have numerous limitations [21] that impacts the performance levels of the network [22]. The reputation and behavior of the node can be used to determine trust values in the trust-based technique. The system has a threshold over which a node is considered normal, and below which it is considered as malevolent [23]. To discover malicious nodes in WSN, a cryptography method is implemented that provides a strong model for node analysis [24].

2. LITERATURE SURVEY

A fuzzy-based solution was presented by Raje and Sakhare [1] in order to increase the security of routing protocols There is a node that employs fuzzy criteria to pick trustworthy routes and uses the trust model for calculating the trust degree of its neighbors. However, the proposed algorithm consumes a lot of energy. In the field of energy-constrained wireless sensor networks, there is definitely a need for further advancements.

A Trust-based Energy Efficient Routing Protocol (TEESR) was introduced by Durrani et al. [3] which relies on suitable permission and flooding methods to prohibit malicious nodes. Node trust values are used to construct coverage area networks and multipath security routes, and then the cluster node and base station node that selects a secure route. Even while the protocol suggested in this paper can deal with convergence holes and wormhole assaults, it can't do anything to stop internal attacks from happening.

Information-Centric Networking (ICN) security requirements were examined by Fang et al. [6] who came up with a Fast and Efficient Trust Management Scheme (FETMS) to resist the On-Off attack. To detect and remove the malicious node responsible for the On-Off attack, FETMS was used. Thus, this system was ideal for low-latency scenarios.

MM-DSR routing protocol is proposed by Frias et al. [7], which works in conjunction with cross-layer algorithms to offer quality of service for various video sources on the network "Reliability Metric (RM)" and "Movement Metric (MM)" are two new parameters defined by the approach. This is by looking at each possible transmission path and picking the best one. These methods rely on the quality of video source; however, they do not ensure that they will work at high speeds.

As a way to improve the DSR routing protocol for MANETs, Sharma et al. [8] proposed a model using ANFIS (fuzzy inference system). Parameters of the ANFIS system take energy, hop count and latency into account when choosing which route information to use to ensure the link can communicate. While this strategy produces ideal pathways, it does not account for the speed of node movement. When nodes move at rapid speeds, the network topology changes dramatically, necessitating the selection of more stable and dependable routes for data transmission.

It is proposed that a Secure Hybrid Routing Protocol (SHRP) based on topography and layering be developed. It consists of two stages, the first two are clustering and cluster head selection, and the second is securing routing methods. Shrp's clustering algorithm is its first step. According to the center position, remaining energy, and node mobility, cluster heads are then selected. The secure routing method, on the other hand, employs symmetric and asymmetric cryptography to protect packets throughout the transmission process against eavesdroppers, impersonation attacks, replay attacks and man in the middle attacks, among other threats. Three GPS nodes are required per cluster. As a result, the protocol's implementation demands a lot of computing and energy. Mezrag et al. [12] proposes a hybrid cryptography-based secure data transfer strategy for wireless sensor networks.

ECC and symmetric key cryptography are introduced in HCBS for key exchange and data encryption, respectively. Viswanathan and Kannan [13] proposed a key management secure routing method based on Enhanced Elliptic Key Cryptosystem Routing Algorithm (ECCSRA) in order to increase the security of the protocol. Because of this, it is impossible for malevolent users to decrypt data using elliptic curve discrete logarithms when the secret key is unknown. Simple prime integers make up the cyclic group utilized in classical elliptic curve encryption. To further enhance network communication security, ECCSRA employs Beta and Gamma functions to produce secret keys.

A Trust and Energy-aware Secure Routing Protocol (TESRP) for WSNs had been proposed by Ahmed et al. [16]. As part of TESRP, nodes exhibiting anomalous behavior are discovered and isolated using a distributed trust model. As a part of its routing approach, TESRP takes into account trust value, residual energy and hops while simultaneously making routing decisions. A significant number of relay nodes must forward RREQ packets in the routing phase, which can lead to congestion of information and increased communication overhead.

A more secure and trusted routing technique is proposed by Beheshtiasl and Ghaffari [18]. The route's trust value is calculated using fuzzy logic. When trust and safety are considered, the shortest route from source to destination is chosen. The MDS-MAP algorithm is used to find the best path with the least amount of errors. According to the trust management system, destination nodes are assumed to be a reliable source of information for the scheme. Many malevolent nodes, on the other hand, might pose as destination nodes to trick genuine nodes to send data.

3. PROPOSED EXTREME TRUST FACTOR FOR ROUTE IDENTIFICATION WITH PRIME NODE MODEL

A wireless sensor network has large nodes that are established dynamically. Each sensor node is capable of communicating sensing and computing information. Sensor nodes deliver data to a base station via wireless transfer mechanisms. A sensor network system, on the other hand, requires a lifetime routing structure [25]. Taking into account the limits, such as the requirement for large capabilities and energy, traditional routing solutions for these networks are ineffective. Routing is very important in WSN nodes [26]. The

routing protocol, also known as a routing policy, specifies how routing mechanisms interact in a network by dividing control data that determines the optimum routes for any two nodes from many routes. In the routing protocol [27], data can be shared from a source node with closer neighbours until it reaches the target node [28]. When routing, it uses algorithms to identify the optimum route between the source and the target node. The proposed model employs Extreme Trust Factor for Route Identification with Prime Node (ETFRI-PN) model to determine the best and most reliable route by taking into account the trusted factors of each and every node involved in the routing process and verifying each node behaviour using a PN node allocated Alphanumeric Inimitable Label. Figure 2 depicts the structure of the suggested model.

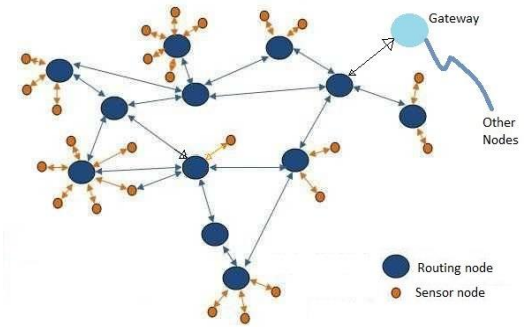

Figure 2. Proposed network structure

3.1 Alphanumeric inimitable label calculation

Cryptography is a set of semantic and mathematical approaches for encrypting data during transmission, particularly in wireless networks. Historically, cryptography was only focused with encryption, or the data transformation from its regular state into an unexplainable and inaccessible state of information using a secret key. The cryptographic method for creating and managing data relies heavily on keys. Every node is assigned an Alphanumeric Inimitable Label (AIL) by the PN node in the proposed scheme. Every node involved in communication will be allotted with a AIL by the PN node. During data transmission, the PN node will monitor the node behaviour using the allocated AIL value.

Algorithm AIL Generation

{

Step-1: Initially a WSN network will be established and the PN node will be selected randomly by considering the computational capabilities and energy levels.

Step-2: Every node sends a request to the PN node to involve in data transmission by sending a ID_REQ message.

Step-3: The PN node will then calculates AIL and then distributes to all the nodes where it got request from. The AIL is calculated by considering two random values X and Y where X is a prime number and Y is not prime and must be greater than X. The ID is allocated for PN node that is calculated as:

$$PN_{Node(i)}[N] = N(i)^{energy(i)_n} \bmod X + Y + Th \qquad (1)$$

Here every node is considered and represented as N(i) and the Th is threshold value considered in the process of ID calculation.

Step-4: The AIL for every node is calculated and then allocated to the requested nodes. The AIL calculation is performed as:

$R_T = X+Y*PN(ID)$

$IK(R_T) = SQRT(R_T)-Th$

$$AIL_{Node(i)} = \frac{\Sigma_{i=1}^{n}\left(X_{N(i)} - Y_{N(i+1)}\right)}{\Sigma_{i=1}^{n} N(i)_i^n \ (\bmod X*Y)^2 + Th} \qquad (2)$$

Here X and Y are 2 random numbers and Alphanumeric Inimitable Label is calculated using the operation.

Step-5: The PN node allots the AIL to all the requested nodes in the network.

}

3.2 Trusted node detection

The trust mechanism in routing includes nodes in routing with strong support on the approximate trust value generated [29]. Trust Calculation is defined as an entity that manages trust relationships, such as acquiring information, making trust-related choices, evaluating trust-related criteria, and observing and re-evaluating existing ties. Tracking neighbour list during transmissions, identifying misbehaviour, assessing trustworthiness based on performance accuracy, and transmitting trust values to finish the routing process are all part of the Trust Calculation process.

Input the number of nodes, initial trust value T and PN node.

Initial node trust level is calculated as:

$$TF_{N(i)} = R_T \sqrt[n]{\prod_{i=1}^{N} T_{i,j,}} node_i$$
$$\in route \sum_{i=1} Max(PDR(i)) + \max(AIL)$$

The PN node will verify the behaviour of each node and then allocates a Status ID (SID). The PN node will allocates SID between 1-50 for malicious nodes and remaining values for normal nodes

3.3 Route detection process

Awareness of the network structure and routing protocol is essential, and it must be suitable for the user requirements [30]. The routing process in the proposed model is represented in Figure 3.

Figure 3 depicts the routing mechanism in the suggested model. Only trusted nodes are considered by the network for commencing data connection.

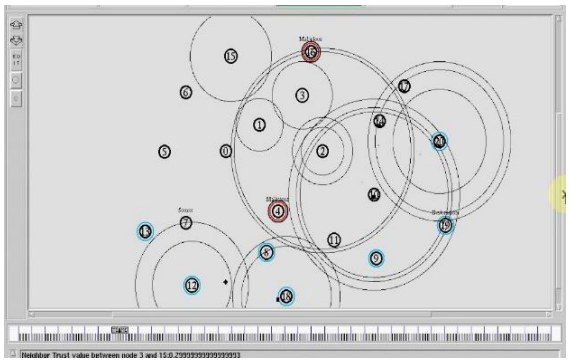

Figure 3. WSN routing in proposed model

The routing protocol is a method for selecting an appropriate route for data to pass from source to destination. While selecting the path, which is dependent on the type of network, channel characteristics, and performance metrics, the process encounters many difficulties. The proposed model considers only trusted nodes to involve in data communication by considering the trust factors of nodes.

Algorithm ETFRI-PN

{

Step 1: Establish a WSN network with the essential nodes to start data transmission.

Step-2: Every node will maintain a routing header with the data indicated as:

$$\text{foreach N(i)} \in \text{WSN(N[])}$$
$$N(i) \leftarrow "TF" + \left|\left(N(i).X - dest.X\right)\right| + \left|\left(N(i+1).Y - dest.Y\right)\right| + AIL(ID)$$
$$route\_table \leftarrow null$$
$$next\_hop \leftarrow null$$
$$Trust\_status \leftarrow null$$
$$dest\_ID \leftarrow null$$

Step-3: The PN node will allocate AILs to the nodes involved in data communication.

$$\text{foreach N(i)} \in \text{WSN(N[])}$$
$$N(i) \leftarrow AIL(N(i)) \leftarrow PN(ID) + Th$$

Step-4: Neighbor nodes will send Node_Trust_Status to the NCH node to verify whether they received the TRREQ message from a trusted node or not.

Step-5: The PN node will verify and update the status to the nodes by allocating the SID after behaviour analysis. The routing header will be finally updated as:

$$\text{foreach N(i)} \in \text{WSN(N[])}$$
$$N(i) \leftarrow "AIL" + \left|\left(N(i).X - dest.X\right)\right| + \left|\left(N(i+1).Y - dest.Y\right)\right|$$
$$route\_table[] \leftarrow Seq(N(i), SID)$$
$$Trust\_status \leftarrow True(>50)$$
$$available\_routes[] \leftarrow Seq(N(i), N(i+1) + Seq(N(j), N(j+1))$$

Step-6: If the node fails to get verified at NCH node level, it is marked as malicious and then removed from the network communication.

$$Malicious\_nodes[] \leftarrow N(i)$$
$$where\ SID < 50$$
$$Trust\_status \leftarrow False(<50)$$

Step-7: The process was repeated until the routing database has been revised from sender to the receiver and all nodes have the status labelled.

Step-8: For data transfer, all available routes are updated, and the route with the highest trust factor nodes is chosen. In the event of a link or node failure, the next possible route is used.

}

4. RESULTS

The proposed model is implemented using NS2 simulator by creating a sensor network and establishing a secured route by considering the trust factors of every node that need to involve in data transmission. The proposed model analyses every node behavior in the wireless sensor network for reducing the malicious actions in the network. The proposed Extreme Trust Factor for Route Identification with Prime Node (ETFRI-PN) model is compared with the existing Software-Defined Multihop Wireless Sensor Networks (SDWSN) Model by considering the factors like Trusted Node Identification Time Levels, Route Detection Accuracy Levels, Route Identification Time Levels, Malicious Nodes in Network, Data Transmission Rate and Route Security Levels. Internet of Things are gaining significance because of its popularity and advantages for achieving quick data transmission and making the humans life easier. Few applications require fast data transmission with minimal interruption, despite the widespread use of sensor networks. The parameters considered for establishing a WSN is indicated in Table 1.

Table 1. Simulation parameters

Parameters	Values
Number of Sensor Nodes	2-50
Simulation Area	1000*1000
Minimum nodes in cluster	20
Initial Energy	100J
Node Energy	100J
Listening Time	1s
Sleep Time	3s
Routing Protocol	Genetic Algorithm

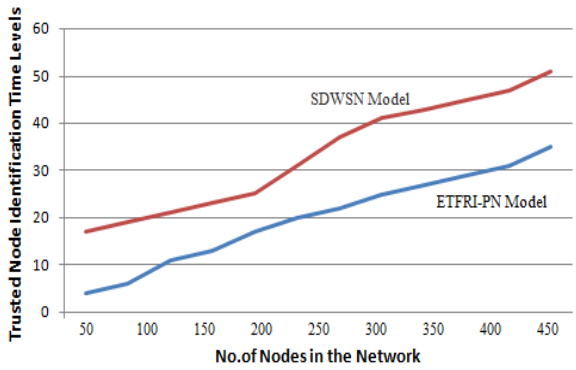

Figure 4. Trusted node identification time levels

The proposed model considers a prime node for monitoring all the sensor nodes that are involved in communication. Based on the trust factor of every node, the nodes are considered as normal nodes or malicious nodes. The trust factors of the nodes will range from 50-100 and the nodes within the trust range are considered as trusted and the remaining are normal or malicious nodes. The proposed model takes less time in identifying trusted nodes. The trusted node identification time levels of the proposed and traditional models are represented

in Figure 4.

Identification of route in the wireless sensor network is a primary task to establish data transmission. The identification of route need to be carefully performed to select only normal nodes and to avoid malicious nodes. The route detection accuracy levels of the proposed model are high as it considers only trusted nodes. A ROUTE REQUEST packet is sent out by a node to initiate a route discovery. Before responding to a ROUTE REQUEST packet, the destination node confirms its originator's identity. The route detection accuracy levels of the proposed and the traditional models are represented in Figure 5.

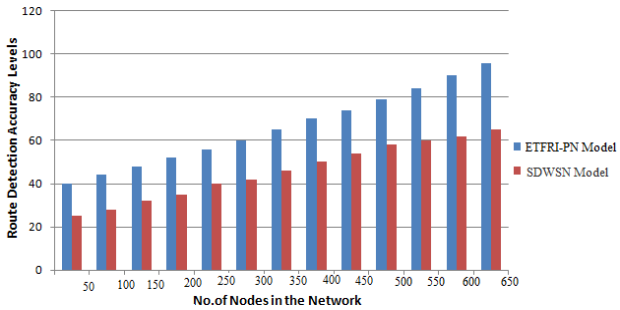

Figure 5. Route detection accuracy levels

Using the routing protocol, data can be routed from source to destination in an efficient manner. It is not easy to choose the route because it is based on the type of network and channel characteristics as well as performance measures. The route identification time levels of the proposed and existing models are indicated in Figure 6.

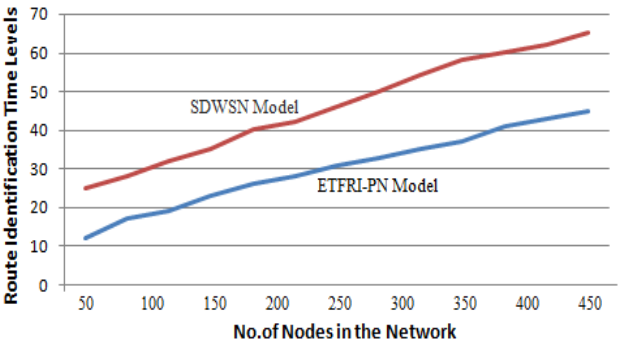

Figure 6. Route identification time levels

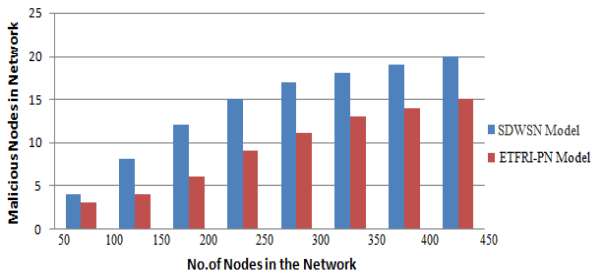

Figure 7. Malicious nodes detection time levels

A malevolent node is one that tries to prevent other nodes in the network from receiving services. A malicious node is one that alters data before, during, or after transmission. The malicious nodes in the network will reduce the network performance levels. The malicious nodes detection time levels of the proposed and traditional models are represented in Figure 7.

The data transmission rate refers to the amount of data sent over a transmission channel or through a data interface in a certain amount of time. Bits per second are the units used for this. The proposed model data transmission rate is high when compared to the existing models. The data transmission rates of the existing and proposed models are shown in Figure 8.

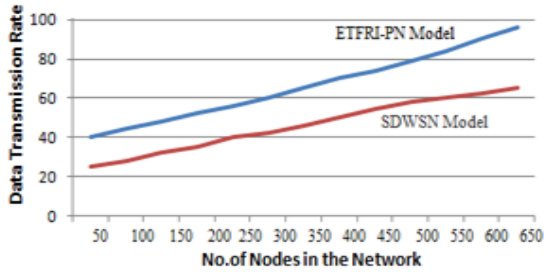

Figure 8. Data transmission rate

The proposed model monitors all the nodes actions in the wireless sensor network to avoid malicious actions. The PN node will monitor all node behavior and then considers them to involve in communication if they are normal. The proposed model route security levels are high than the existing model. The Figure 9 represents the route security levels of both existing and proposed models.

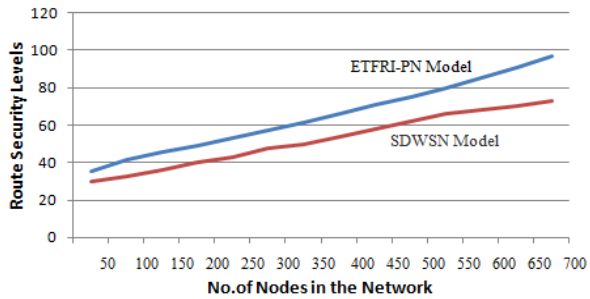

Figure 9. Route security levels

5. CONCLUSION

Secure routing is critical for the acceptability and deployment of sensor networks in many applications, however based on the survey done, it is observed that the routing protocols currently available are insecure. Routing in sensor networks is a relatively recent field of study, with a small but rapidly developing body of knowledge. Transmission of data is processed and measured in a wireless sensor network in order to ensure data security while being transmitted between the intra nodes in the network. On the basis of node behavioral changes, it aims to solve the problem of normal nodes being isolated in practical communication. The proposed model considers a PM node that analyzes the node behavior and identifies a trust factor. Based on the trust factor, the node behavior is analyzed and marked as normal node or malicious node. The packet delivery rate of the proposed model is enhanced as the malicious nodes will be easily detected that results in performance enhancement. As the malicious nodes are identified based on their behavior and historical performance, rather than demanding all the nodes in a path, as

is done in traditional methods, the improvisation is possible, which helps to keep the network alive for longer time and increase the performance. By studying the semantic changes in the negative and positive messages spread by intermediate nodes as well as malicious nodes, we hope to develop a more stable network over the network in the future. In future, the cryptography models complexity levels can be reduced to enhance the performance levels.

REFERENCES

[1] Raje, R.A., Sakhare, A.V. (2014). Routing in wireless sensor network using fuzzy based trust model. In 2014 Fourth International Conference on Communication Systems and Network Technologies, pp. 529-532. https://doi.org/10.1109/CSNT.2014.111

[2] Wang, J., Li, L., Chen, Z. (2011). A routing algorithm based on trustworthy core tree for WSN. In: IEEE/IFIP International Conference on Embedded & Ubiquitous Computing. Hong Kong, China. pp. 763-770. https://doi.org/10.1109/EUC.2010.120

[3] Durrani, N.M., Kafi, N., Shamsi, J., Haider, W., Abbsi, A.M. (2013). Secure multi-hop routing protocols in Wireless Sensor Networks: Requirements, challenges and solutions. In Eighth International Conference on Digital Information Management (ICDIM 2013), pp. 41-48. https://doi.org/10.1109/ICDIM.2013.6694001

[4] Senthil, T., Kannapiran, B. (2017). ECTMRA: Energy conserving trustworthy multipath routing algorithm based on cuckoo search algorithm. Wireless Personal Communications, 94(4): 2239-2258. https://doi.org/10.1007/s11277-016-3378-6

[5] Sun, B., Li, D. (2017). A comprehensive trust-aware routing protocol with multi-attributes for WSNs. IEEE Access, 6: 4725-4741. https://doi.org/10.1109/ACCESS.2017.2786944

[6] Fang, W., Xu, M., Zhu, C., Han, W., Zhang, W., Rodrigues, J.J. (2019). FETMS: Fast and efficient trust management scheme for information-centric networking in Internet of Things. IEEE Access, 7: 13476-13485. https://doi.org/10.1109/ACCESS.2019.2892712

[7] Frias, V.C., Delgado, G.D., Ayala, A.Z., Igartua, M.A. (2007). MM-DSR: Multipath QoS routing for multiple multimedia sources over ad hoc mobile networks. IEEE Latin America Transactions, 5(6): 448-456. https://doi.org/10.1109/TLA.2007.4395234

[8] Sharma, V., Alam, B., Doja, M.N. (2019). An improvement in DSR routing protocol of MANETs using ANFIS. In Applications of Artificial Intelligence Techniques in Engineering, pp. 569-576. https://doi.org/10.1007/978-981-13-1822-1_53

[9] Yang, H., Liu, Z. (2019). An optimization routing protocol for FANETs. EURASIP Journal on Wireless Communications and Networking, 2019(1): 1-8. https://doi.org/10.1186/s13638-019-1442-0

[10] Preetha, K.G., Unnikrishnan, A. (2017). Enhanced domination set based routing in mobile ad hoc networks with reliable nodes. Computers & Electrical Engineering, 64: 595-604. https://doi.org/10.1016/j.compeleceng.2017.04.028

[11] Arafat, M.Y., Moh, S. (2018). A survey on cluster-based routing protocols for unmanned aerial vehicle networks. IEEE Access, 7: 498-516. https://doi.org/10.1109/ACCESS.2018.2885539

[12] Mezrag, F., Bitam, S., Mellouk, A. (2017). Secure routing in cluster-based wireless sensor networks. In GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1-6. https://doi.org/10.1109/GLOCOM.2017.8254138

[13] Viswanathan, S., Kannan, A. (2019). Elliptic key cryptography with Beta Gamma functions for secure routing in wireless sensor networks. Wireless Networks, 25(8): 4903-4914. https://doi.org/10.1007/s11276-019-02073-9

[14] Harn, L., Hsu, C.F., Ruan, O., Zhang, M.Y. (2015). Novel design of secure end-to-end routing protocol in wireless sensor networks. IEEE Sensors Journal, 16(6): 1779-1785. https://doi.org/10.1109/JSEN.2015.2504375

[15] Umar, I.A., Hanapi, Z.M., Sali, A., Zulkarnain, Z.A. (2017). Trufix: A configurable trust-based cross-layer protocol for wireless sensor networks. IEEE Access, 5: 2550-2562. https://doi.org/10.1109/ACCESS.2017.2672827

[16] Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W., Haseeb, K. (2017). Energy-aware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Networking and Applications, 10(1): 216-237. https://doi.org/10.1007/s12083-015-0421-4

[17] Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W. (2016). A secure routing protocol with trust and energy awareness for wireless sensor network. Mobile Networks and Applications, 21(2): 272-285. https://doi.org/10.1007/s11036-016-0683-y

[18] Beheshtiasl, A., Ghaffari, A. (2019). Secure and trust-aware routing scheme in wireless sensor networks. Wireless Personal Communications, 107(4): 1799-1814. https://doi.org/10.1007/s11277-019-06357-3

[19] Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., Ding, Q. (2017). Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access, 5: 9599-9609. 10.1109/ACCESS.2017.2706973

[20] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110(4): 1637-1658. https://doi.org/10.1007/s11277-019-06788-y

[21] Ishaq, Z., Park, S., Yoo, Y. (2015). A security framework for cluster-based wireless sensor networks against the selfishness problem. In 2015 Seventh International Conference on Ubiquitous and Future Networks, pp. 7-12. https://doi.org/10.1109/ICUFN.2015.7182485

[22] Bilgin, B.E., Baktir, S. (2019). A light-weight solution for blackhole attacks in wireless sensor networks. Turkish Journal of Electrical Engineering & Computer Sciences, 27(4): 2557-2570. https://doi.org/10.3906/elk-1809-23

[23] Liu, Y., Dong, M., Ota, K., Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9): 2013-2027. https://doi.org/10.1109/TIFS.2016.2570740

[24] Fang, W., Zhang, W., Chen, W., Liu, J., Ni, Y., Yang, Y. (2021). MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2021(1): 1-20.

https://doi.org/10.1186/s13638-020-01884-1
[25] Yu, X., Li, F., Li, T., Wu, N., Wang, H., Zhou, H. (2020). Trust-based secure directed diffusion routing protocol in WSN. Journal of Ambient Intelligence and Humanized Computing, pp. 1-13. https://doi.org/10.1007/s12652-020-02638-z
[26] Rathee, M., Kumar, S., Gandomi, A.H., Dilip, K., Balusamy, B., Patan, R. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management, 68(1): 170-182. https://doi.org/10.1109/TEM.2019.2953889
[27] Saidi, A., Benahmed, K., Seddiki, N. (2020). Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks. Ad Hoc Networks, 106: 102215. https://doi.org/10.1016/j.adhoc.2020.102215
[28] Thangaramya, K., Kulothungan, K., Indira Gandhi, S., Selvi, M., Santhosh Kumar, S.V.N., Arputharaj, K. (2020). Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. Soft Computing, 24(21): 16483-16497. https://doi.org/10.1007/s00500-020-04955-z
[29] Isaac Sajan, R., Jasper, J. (2020). Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network. International Journal of Communication Systems, 33(8): e4341. https://doi.org/10.1002/dac.4341
[30] Laxmi, B.P., Chilambuchelvan, A. (2017). GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks. Future Generation Computer Systems, 76: 98-105. https://doi.org/10.1016/j.future.2017.05.015