Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.026465
Article

Enhanced Security with Improved Defensive Routing Mechanism in Wireless Sensor Networks

R. Sabitha[1,*], C. Gokul Prasad[2] and S. Karthik[1]

[1]Department of Computer Science & Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India
[2]Department of Electronics and Communication Engineering, SNS College of Engineering, Coimbatore, Tamilnadu, India
*Corresponding Author: R. Sabitha. Email: dr.r.sabitha@gmail.com
Received: 27 December 2021; Accepted: 25 March 2022

Abstract: In recent scenario of Wireless Sensor Networks (WSNs), there are many application developed for handling sensitive and private data such as military information, surveillance data, tracking, etc. Hence, the sensor nodes of WSNs are distributed in an intimidating region, which is non-rigid to attacks. The recent research domains of WSN deal with models to handle the WSN communications against malicious attacks and threats. In traditional models, the solution has been made for defending the networks, only to specific attacks. However, in real-time applications, the kind of attack that is launched by the adversary is not known. Additionally, on developing a security mechanism for WSN, the resource constraints of sensor nodes are also to be considered. With that note, this paper presents an Enhanced Security Model with Improved Defensive Routing Mechanism (IDRM) for defending the sensor network from various attacks. Moreover, for efficient model design, the work includes the part of feature evaluation of some general attacks of WSNs. The IDRM also includes determination of optimal secure paths and Node security for secure routing operations. The performance of the proposed model is evaluated with respect to several factors; it is found that the model has achieved better security levels and is efficient than other existing models in WSN communications. It is proven that the proposed IDRM produces 74% of PDR in average and a minimized packet drop of 38% when comparing with the existing works.

Keywords: Enhanced security model; wireless sensor networks; improved defensive routing mechanism; secure paths; node security

1 Introduction

Due to the rapid growth of Internet of Things (IoT) and the services of wireless sensor networks, the methodologies for secure communications over the network acquire more attention. The efficient features of sensor networks such as cheaper nodes, fast node deployment and self organization of nodes plays an important role in framing efficient network and provides smart communication environment. Moreover, the omnipresent sensor nodes can acquire physical data of the deployed environment and administrate the environment [1]. In the limited range of wireless network communications, the data transmission can be

effectively made through the multi hop path transmission. In such scenario, the model of secure routing protocol that establishes the data transmission path is a significant process that impacts the wireless sensor network performance effectively [2–4]. The general framework of secure WSN is presented in the Fig. 1.

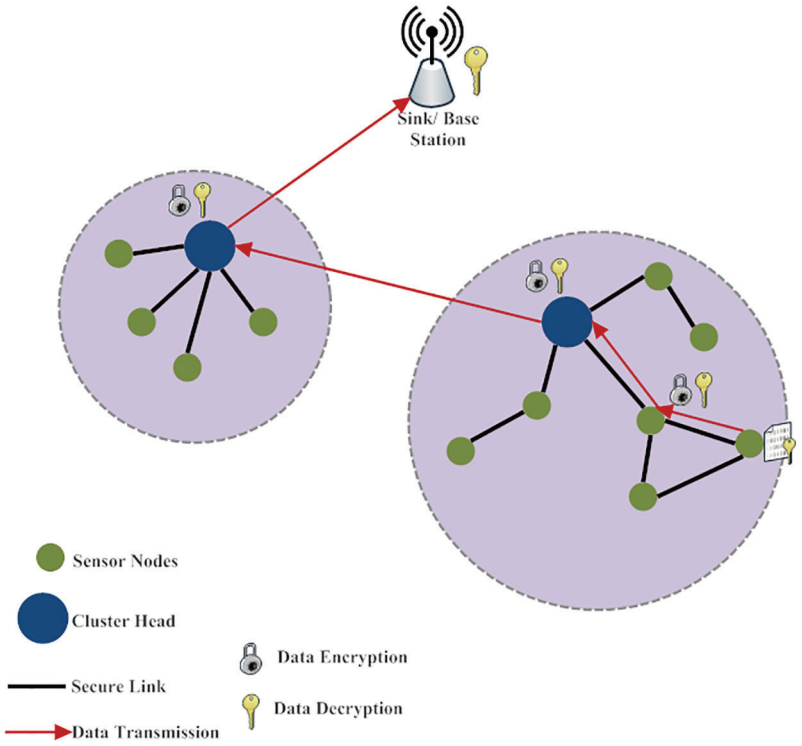

Figure 1: General framework of secure wireless sensor network model

In this paper, the security factors are mainly considered to design an efficient routing protocol in Wireless Sensor Networks. The WSNs are open to various attacks, because of their typical features such as, distributed nature, openness and adaptive feature of networks [5,6]. In general, the attacks in WSN can be categorised into, internal and external, which affects the network communications through the malicious nodes [7,8].

In recent days, there are several models have been developed to solve the security issues and present mitigation techniques [9,10]. For enforcing security, cryptographic techniques are used. In utilizing the cryptographic primitives, two factors are to be considered as follows [11,12],

i) The cryptographic functions need higher computational complexities
ii) Many encryption techniques requires central admin to control, which is not applicable in WSN
iii) When the nodes are distributed in unattended region they could be attacked by attackers easily.

On focussing the above aspects, developing a model with defending mechanism and trust management provides optimal solution [13]. For determining the secure route effectively, the trust management based evaluations aids to find the security factor of the sensor at next-hop through which the data is transmitted from the source node to the base station. In conventional methods of securing WSN, there exists several key based issues in routing. Moreover, in designing a new model for secure WSN communications, the Quality of Service (QoS) parameters such as the transmission delay, hop counts are to be considered. Models incorporating trust management in WSN, includes trust evaluations and derivations for proper

execution. Trust evaluations acquire more focus than the other, in which the trust data is shared often for assuring efficiency of the trust computations. But, in some cases, the trust management enforcing in WSN is registered as a complicated process. In this work, an Enhanced Security Model with Improved Defensive Routing Mechanism (IDRM) is proposed to solve the limitations in providing security over wireless sensor network communications. Here, optimal secure paths and Node security levels are evaluated for effectively dealing with attacks and defending the sensor communications. Moreover, the defensive routing is framed by deriving mathematical computations. In the process of optimal secure path determination, are considered the parameters of trust management along with the quality of services. It is observed from the proposed model, that the model provides complete secure data transmission and also minimizes the routing overhead in an effective manner.

The remaining part of this paper is framed as follows: Section 2 contains a brief explanation on the existing security model in wireless sensor networks. Section 3 discusses about the possible various attacks in WSN. The proposed model is clearly described with pictorial representations in Section 4. Section 5 presents the result evaluations and comparative analysis for evidencing the efficacy of the proposed work. Finally, the conclusion and future works are presented in Section 6.

2 Related Work

In [14], Secure aware Ad-hoc Routing protocol called SAR has been developed for determining the secure and optimal path with required security parameters. The sensor at the source determines the required security standards for the effective route determination. The sensors with similar security standards could share the encryption keys and decryption has been done with the secured packet. SAR protocol transmits the message to the destination by means of route discovery in a secure manner. But the major drawback is that the discovered path is not shortest path to the destination. The results of SAR are depicted only during the absence of attack. The cryptographic primitives used in the model might cause encryption overheads. Additionally, with the application of encryption techniques, the internal attacks made with the malicious and compromised nodes could not be handled effectively [15].

Based on the increasing requirements of security primitives, trust management based protocols have been developed in [16–18]. In [19], a model has been derived based on the Bayesian gaming approach to defend the network from Denial of Service attacks. Moreover, LEACH based routing protocol has been used for communications, but, the process was not effective in dealing with attacks. In the works of [20–22], an informative review work has been done, about the attacks and trust model against those attacks. Moreover, the paper narrated variety of attacks and mitigation techniques for secure routing in WSN.

In the work presented in [23], the authors discussed about the trust metrics for secure WSN with some mathematical evaluations. Further, a distributed trust model has been proposed in [24]. The bootstrapping phase of the model was handled with secret dealer, which may restrict the WSN features to be feasible for applications. Further, in [25], Trust based Secure Routing (TSR) has been developed to predict and frame the trust model based on the behaviour analysis of the sensor nodes that are involved. It was observed from the result evaluations that the trust evaluation model was not so accurate, since the nodes determine shortest secure route for packet transmission and here the average trust rate of all nodes was not considered. Moreover, the trust of sensors was evaluated by analyzing both the direct and indirect trust computations in [26]. When applying the model in real time scenarios, only few attacks could control the general attacks and the routing overhead could not be reduced. In [27], a trust based secure routing has been defined for MANET to effectively share resources in the network. Jamming Attack is a type of DoS attack which is also one of major threat that should be avoided. In [28] three techniques have been used for preventing jamming attacks. In [29], the authors have majorly concentrated towards the detection of black hole attack by means of Modified Associativity Based Routing (MABR) protocol.

In [30], a block chain-based authentication is used for secure data transmission in which trust value of each node is computed and hence the results have proven to have reduced delay in packet transmission and higher packet delivery ratio. Here, a major concern is on intra-network and they didn't focus towards the inter-network.

Trust Evaluation Mechanism is opted to ensure the security of the network at a lower cost. Trust of each node is evaluated followed by a reasonable reward and a competent path determination between the source and the destination node in [31]. The major drawback of this work is its efficiency and excellence of collecting the data. In [32,33], the authors have used trust evaluation for securing the data transmission where, in specific, they eliminated the selfish nodes using the vitality of the nodes and their control messages.

Among the papers reviewed all the authors have equally used cryptographic and trust evaluation for securing the transmission of data in the network. The performance of the network is much better when evaluating the trust rate of the nodes. Thus, we have used trust evaluation for data transmission in WSN.

3 Various Attacks in WSN

Design of Routing protocols is the most important function in the wireless sensor network communications, since it decides the data transmission flow throughout the network. Nevertheless, in many conventional models of routing consider that the environment is secure and no security problems are there. But, the assumption cannot be applicable in several cases, because of the openness of the WSN environment, the network is vulnerable to several attacks such as, Sybil attacks, black hole, wormhole attacks and so on [34]. Subsequently, secure data transmission is very significant to assure the network operations for handling malicious nodes. For framing secure and efficient data transmission model, several attacks are analyzed and listed as follows,

A. Blackhole Attack:

A malicious or compromised node discards the data packets transmitted through the node. This attack drops all received packets which are intended for forwarding. This attack will degrade the performance of the network. If we employ different routes from source to destination this attack be eliminated.

B. Greyhole Attack:

It is an advanced transformation of the blackhole attack. This attack involves in dropping certain packets and transmits only partial data to the destination. Furthermore, it reduces the efficiency of the networks.

C. Sinkhole Attack:

The overall network traffic is acquired using a compromised node and the node itself acted as a sink node for getting the sensed data. It is one of the sternest routing attacks because it attracts the surrounding nodes with misleading routing path information and performs data forging or selective forwarding of data passing through it. It can cause an energy drain on surrounding nodes resulting in energy holes in WSNs and it can cause inappropriate and potentially dangerous responses based on false measurements.

D. Wormhole Attack:

In this, a set of attackers pass the packets that is acquired at the one terminal of the network and transmit through another terminal with a low latency communication link. Here, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many *ad hoc* network routing protocols and location-based wireless security systems.

E.Sybil Attack:

In this attack, a node illegally provides multiple identities to other sensors in the defined network, which interrupts the reliable packet transmission. It is one of the biggest issues when connecting to a P2P network. It manipulates the network and controls the whole network by creating multiple identities.

F. Denial of Service Attack:

In order to interrupt the communication, flooding is caused by the attacker with false or redundant traffic. By this attack, genuine users are not able to access resources, so may not be able to find the information or carry out the actions they need. They may suffer reputational damage.

G. Sniffing Attack:

The sensed data is eavesdropped by an attacker. A sniffing attack involves the illegal extraction of unencrypted data by capturing network traffic through packet sniffers. This type of attack can be eliminated if we avoid transmissions through unsecured network, proper network scanning and routing.

H. Message Tampering:

The original data to be transmitted through the network is tampered before transmitting to other nodes. This type of attack can be eliminated by employing encryption mechanisms and network monitoring.

I. Replay Attack:

A replay attack is also known as a playback attack. It help attackers to gain access to a network, gain information which would not have been easily accessible or complete a duplicate transaction. Instead of transmitting the original sensed data, the attacker makes the repeated forwarding of earlier packets.

Further, trust management based common attacks in wireless sensor networks are illustrated below.

a. On-off Attacks:

The malicious nodes are active and inactive alternatively to remain in the trusted networks.

b. Conflicting behaviour attack:

For compromising the network, the malicious nodes perform variety of behaviour for different set of nodes.

c. Bad Mouthing Attack:

A malicious node provides false recommendations and broadcasts the recommendation data based on the behaviour of the malicious nodes.

d. Collusion Attack:

In this attack, one or more malicious node colludes with another to interrupt the network functionalities.

4 Proposed Model

In the proposed IDRM model, network is designed with some aggregation nodes (AN) and randomly deployed sensor nodes (SN) in a defined region. Each SN in the network has the responsibility of defending attacks and transmitting data packets. It is also to be considered on designing the network model; the nodes in the network have limited resources and similar communication ranges. Additionally, communication among typical wireless sensor network happens through multi-hop data transmission, where the communication model is designed in distributed mode. It is also assumed in the network that the nodes can be compromised by various attackers, when no security model is properly defined for

communications. Since, the nodes are acquired from different service providers, the selfish nodes may not effectively collaborate with others.

4.1 Definition of System Model

In order to evaluate the routing problems in wireless sensor networks, graph model is used for defining the system effectively. The, Weighted Directed Graph is denoted by *WG(V, L, wt)*, where, 'V' represents the set of nodes deployed in the network, '$L \subseteq V \times V$' is the link set of the distributed sensors and 'wt' denotes the weight factor that is used to measure the paths between nodes. For each *l(a,b)* $\in L$, in which, node 'i' is the source and node 'j' is the destination node. Therefore, the route 'R' from V_1 to V_n is states as follows,

$$R(V_1,\ V_n) \triangleq (V_1, V_2,\ \ldots V_n) \tag{1}$$

In this proposed IDRM, each SN is responsible for tracking its own neighbour behaviours and measuring their trust model for designing an effective security level for communications. The trust rate of the node 'b' for sensor 'a' is given as 'TR *(a, b)'*, in which the sensor node 'a' involves in evaluating the security level of node 'b' for forwarding the data packets. In specific, 'TR' of any random node in the network contains primary trust (pt) and secondary trust (st). Here, the primary trust is defined as the trust level acquired by direct monitoring of any node that is involved in the process of data transmission. On the other hand, secondary trust is defined as the trust obtained through the references from other nodes.

For defining enhanced and secure routing model, two graphical structures are considered, which are given as follows,

$$Physical\ Graph \rightarrow WG_P(V,\ L_P,\ \alpha) \tag{2}$$

$$Routing\ Graph \rightarrow WG_R(V,\ L_R,\ \beta) \tag{3}$$

In (2), 'L_P' represents the set of directed physical paths, whereas in (3), it denotes the efficient route determination for data transmission. In this work, 'α' is weighted label that represents the parameter used for route measurement and routing parameter 'β' is combined metric of trust and other quality of service factors, which is used in 'WG_P' for defining the physical link effectively. Moreover, the proposed Improved Defensive Routing Mechanism defines an optimal path with enhanced QoS and the assurance of secure data transmission.

4.2 Node Security Based Trust Evaluations

With the consideration of resource constraints of sensor nodes such as limited power, memory, energy and bandwidth, the model has derived a lightweight evaluation model or trust computations.

$$TR\ (a,b)^s = \gamma \times pt(a,b)^s + \delta \times \frac{\sum_{m \in N_b,\ m \neq a}^{n} st(m,\ b)^s}{n-1} \tag{4}$$

In the above Eq. (4), 'γ' and 'δ' are weight parameters with respect to security policies of nodes, those values are not greater than 0, and N_b denotes the neighbour sensor set of node b. Moreover, 'n' is the number of neighbour_nodes and 's' denotes the sequence order of the computed data. When the parameter 'γ' attains higher value, the specific SN is convincing about its own decisions, whereas, the larger value of 'δ' states that the trusted nodes referred by other nodes can be believed. The value obtained for TR must be higher for defining the node to be more secure. By fixing appropriate values to the weight parameters, the conflicting attacks can be avoided effectively. By observing the node behaviours using the neighbour nodes, the nodes that behaves in differently on malicious nodes can be detected effectively. The detection process can be effectively performed by the combined computations of primary trust and secondary trust values. The calculation for determining the primary trust value is given as,

$$pt(a,b)^s = \rho_1 \times pt_{p(b)}(a,b)^{s-1} + \rho_2 \times pt_{N(b)}(a,b)^{s-1} + IDF(a,b)^s \tag{5}$$

In the above equation, '$pt_{p(b)}(a,b)^{s-1}$' denotes the directly monitored trust rate of node 'b' for node 'a' based on the previous behaviours of the node and '$pt_{N(b)}(a,b)^{s-1}$' represents the malicious behaviour of node. 'ρ_1' and 'ρ_2' are the decay time metric of positive and negative evaluations respectively. Intrusion Detection System based behaviour analysis is presented as '$IDF(a,b)^s$'. It can be mathematically defined as,

$$Intrusion\ Detection\ Factor(IDF) = \begin{cases} P(b), & lies\ between\ 0\ and\ 1 \\ N(b), & lies\ between\ -1\ and\ 0 \\ 0, & for\ uncertain \end{cases} \tag{6}$$

Here, 'P(b)' and 'N(b)' denotes the positive and negative behaviour of node 'b'. Further, the secondary trust value of nodes in security evaluation process is given as,

$$\sum\nolimits_{(m\in N_b,\ m\neq a)}^{n} st(m,\ b)^s = \sum\nolimits_{(m\in N_b,\ m\neq a)}^{n} pt(a,m)^s \times pt(m,b)^s \tag{7}$$

4.3 Determination of Secure Paths

When a source SN is ready to forward data packets to the destination SN, a secure path must be selected for packet forwarding. For determination of secure path, it is to be considered that the trust rate of the path should be lesser than the trust rate of the intermediate SN in the path. It is also to be assumed that the destination SN must be a secure node, should be trusted for data forwarding. Moreover, the trust rate (TR) for any other SN is assumed to be 1. The trust rate of the path is computed by the greatest product result of all the TRs over the path. The mathematical computation of the secure Route (SR) is given as,

$$TR(SR) = \prod(\{TR(a,b)|a,b \in SR, a \rightarrow b\}) \tag{8}$$

Here, SNa and SNb are considered as neighbours. The secure path determination is clearly given in the Fig. 2, in which, the SN0 is considered as source and the SN5 is assumed as the destination node. Among the sensor node set {SN0, SN1, SN2, SN3, SN4, SN5}, the TR of possible routes from source to destination are given as,

$$TR \rightarrow \begin{cases} \{SN_0, SN_3, SN_4, SN_5\} = 0.48 \\ \{SN_0, SN_1, SN_2, SN_5\} = 0.72 \\ \{SN_0, SN_3, SN_2, SN_5\} = 0.56 \end{cases}$$

Among the possible paths from the source to destination, the path having the most maximum TR is selected for packet transmission. In this, the secure path determination with maximum TR can be derived as,

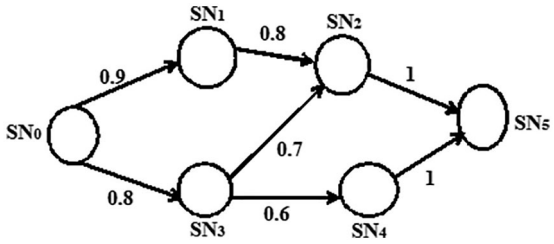

Figure 2: Sample case for secure path determination

$$TR(SR) = \max(\{TR(a,b)|a,b \in SR, a \rightarrow b\}) \quad (9)$$

The above described function, max () provides the maximum trust rate of routes and in the sample scenario presented in the above Fig. 3, TR $\{SN_0, SN_1, SN_2, SN_5\}$ contains maximum TR, which is considered as the secure route among others. The complete work flow of the proposed model is presented in Fig. 3.

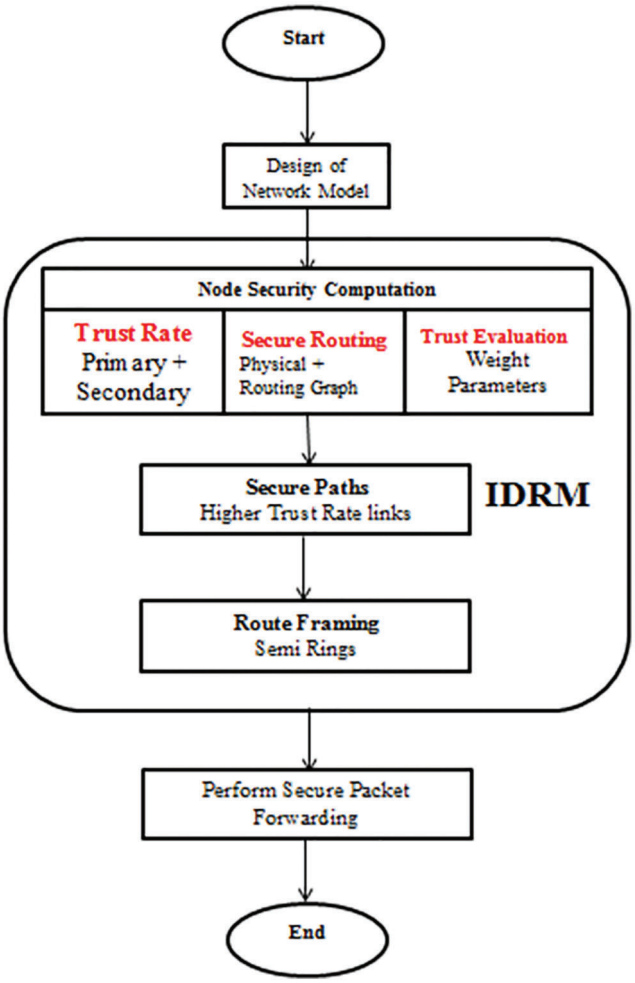

Figure 3: Workflow of proposed IDRM

4.4 Complete Route Framing In Idrm

Here, the complete route framing of Improved Defensive Routing Mechanism is implemented with the semi-rings concept. When there is a need of choosing an optimal secure path, $P(SN_0, SN_n)$, optimal route is framed as,

$$P^*(SN_0,\ SN_n) = \oplus_T[TR(P(SN_0,\ SN_m)) \otimes_{T(TR)} (P(SN_m, SN_n))] \quad (10)$$

where, $m \in (SN_0,\ SN_n)$ and TR is computed from the Eq. (8), which is presented in Section 4.3. Moreover, operator '$\oplus_T$' denotes the maximum value of the function and '$\otimes$' denotes the product functions. The path determination for routing with lower delay can be given as,

$$P^{*}\ (SN_0,\ SN_n) = \oplus_{LD}[TR(P(SN_0,\ SN_m))\otimes_{LD(TR)}(P(SN_m, SN_n)] \tag{11}$$

In which, 'LD' denotes the lower delay computation of optimal route that denotes the minimal function description. The routing algorithm is framed with respect to the distinctive routing requirements. IDRM algorithm is given in the Tab. 1.

Table 1: Algorithm for improved defensive routing mechanism (IDRM)

Begin

Initialize Weighted Graph for network model

$SN_n \rightarrow$ destination node, SN Source Node

Append SN_n to SN* list, where SN* denotes set of optimal route to reach SN_n

While $SN_i \neq SN^*$, SN_i denotes set of all nodes in the network

$\forall\ SN \in SNi - SN^{*}$ do

Compute

$\overrightarrow{SR}\,(P(SN_i, SN_n)) \underset{=}{\triangle} (R_0,\ R_1,\ \ldots, R_m)$, where R_0 is the trust degree and $R_{1,..}R_m$ is the Quality metrics

$\forall$ *sensor node* $SN_i \in\ C(SN)$, where C(SN) – set of nodes that can be used in communication to reach SN_n

If $TR(SN, SN_i)\otimes_{pt(TR)}(P(SN_i, SN_n)) \geq THR(P(SN, SN_n))$ then

Add $(SN,\ P(SN_i, SN_n))$ to P to the Route set $SR^{*}(SN, SN_n)$

End if

End for

If $SR^{*}{}_{Ri}(SN, SN_n) = \varnothing$ then

SN is left the network

End if

For k = 1;k < m;k++ do

$SR^{*}{}_{Rj}(SN_i, SN_n) = \oplus_{Rj} SR^{*}{}_{Rj-1}(SN_i, SN_n)$

End for

If $SR^{*}{}_{Rj}(SN, SN_n) = \varnothing$ then

SN is left the network

Continue;

Else

Add SN_i to SN*

Add $SR^{*}{}_{Rj}(SN_i, SN_n)$ to $WG^{*}_{SR}(SN,\ L_{SR},\ sr)$

End if

End for

End while

End

Based on the above algorithm, implementation of IDRM is carried out in the defined heterogeneous wireless sensor networks. The establishment of the proposed model is done with the considerations of resource limitations of nodes in the wireless sensor networks. Figs. 4A–4C depicts the route framing process using the basic handshake based communication process for transmitting packet from Sensor node SN_1 to SN_{10} (*i.e.*, source to destination, which are considered as trusted nodes initially). The steps involved in the implementation process are explained below.

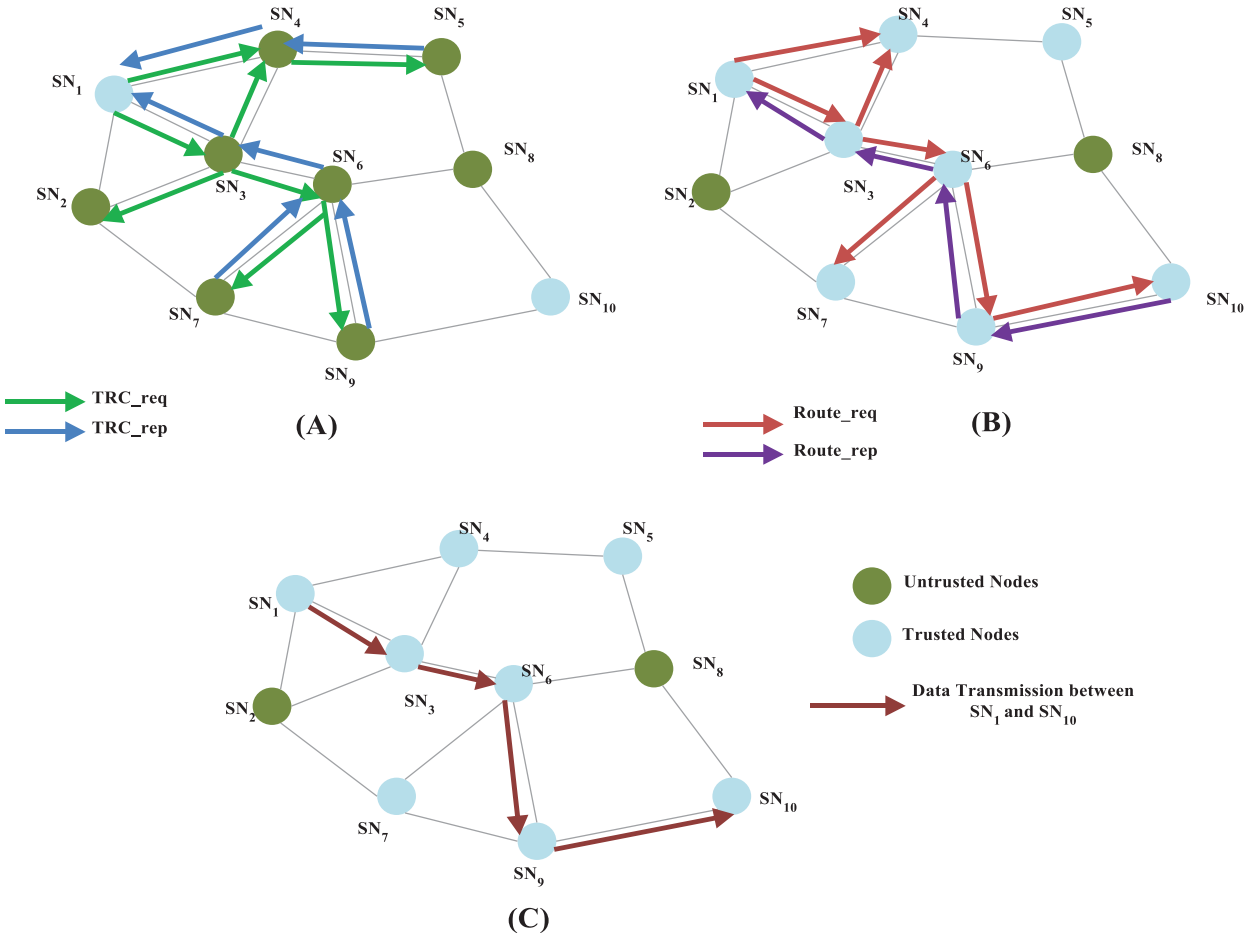

Figure 4: Process of improved defensive routing

1. When the node 'SN_1' is ready to forward data packets to the sensor node 'SN_{10}', the source node begins the process of IDRM. Initially, TR computation request is sent to all nodes that includes TRC_req =< S_{id}, T_{id}, thresh, TS, N, HC>, in which, 'S_{id}' represents the identity of the node presently evaluating, 'T_{id}' denotes the ID of evaluated nodes, threshold value of TR, timestamp (TS), 'N' denotes the sequence number, and 'HC' is the hop count.
2. On receiving the TRC_req, the trust rate of each neighbour node is evaluated and based on that TR_rep is unicasted from the neighbour nodes that received the request.
3. After acquiring the references given by the neighbour_nodes, the source node derives the TR of remaining nodes based on the primary and secondary trust evaluations, and the route_req is forwarded to the nodes.

4. When the adjacent most trusted sensor receives the route_req, the route_rep will be sent to the source. In this way, the optimal secure route will be framed from source to destination.
5. Once the route_req reaches the destination node, the route_rep will be sent to the source by the route obtained by the Algorithm given in Tab. 1.
6. Finally, the data packets are forwarded through the determined secure route that is capable of defending attacks, from source to destination.

For any routing algorithm, it is important to define the process of route maintenance. When a new sensor node joins the defined network model, the behaviour of the new node is observed by its neighbour_node. Further, the process of TR derivation is carried out based on the route request received for data transmission. When reply message is received based on the trust rate of the path and the node, the sensor is considered for new route formation.

5 Result and Discussion

The experimentation is carried out in Network Simulator-2 (NS-2) tool. Moreover, it is considered that the network model contains 500 sensor nodes that are deployed in 500 × 500 m^2. Here, the comparative evaluations have been made with the existing models such as SAR and TSR. For the purpose of the proposed model evaluations, the deployed nodes are considered as two parts, namely, malicious nodes and well-behaved nodes. The IDRM is compared with 2 other existing works: the first one is SAR (Secure Aware Ad-Hoc Routing Protocol) which was used route discovery for data transmission by means of RREQ and RREP message where the path to destination was not the shortest path and the results was proven without attacks. Second one is TSR (Trust-Based Secure Routing Protocol) which is based on trust evaluation which gives a better performance in terms of packet delivery ratio and end-to-end latency. They didn't concentrate towards load and delay of the route. The IDRM is proposed to give a better performance in terms of trust evaluation which is much better than the other cryptographic techniques in providing the security while transmitting data. The performance results are evaluated based on Packet Delivery Ratio (PDR), Routing Overhead, Packet Drop, Throughput, and Transmission Delay.

In order to test the efficiency of IDRM, the initial setting on the simulation tool is given in Tab. 2. With the above initial settings, the results are evaluated based on the performance metrics such as packet delivery rate, routing overhead, transmission delay, packet drop and throughput.

Table 2: Initial simulation settings

Parameters	Initial values
Sensing area	500 × 500 m^2
Simulation area	500 s
Number of sensor nodes	500
Communication range	40 m
Interval in packet forwarding	5 s
Size of packet	100 bytes
Initial trust rate (TR)	0.5
Error detection probability	0.1
Presence of malicious nodes	30%

In Fig. 5, the average packet delivery rate of model is analysed and the results are compared. It is observed from the Fig. 5 that the proposed model defends the malicious node, which is assumed to be in 30% in the defined model, and has produced 74% of PDR in average. Here, the result of PDR is 32% greater than the other existing models. For sample cases, in Figs. 6 and 7, two common attacks such as Tampering Attack and On-Off Attack are considered to be interrupting the process of packet forwarding between the source and destination, respectively.

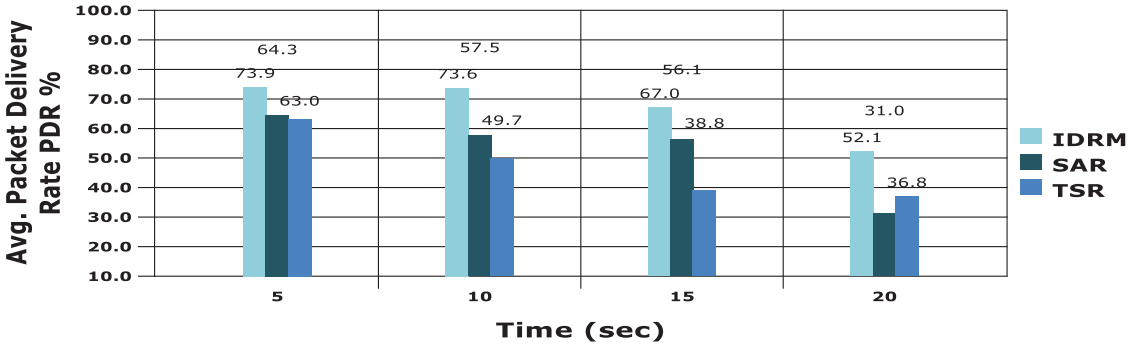

Figure 5: Evaluation of packet delivery rate among models

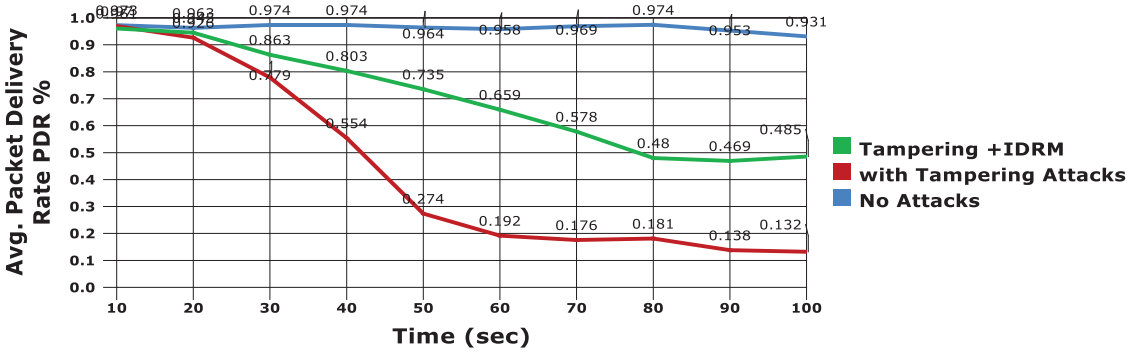

Figure 6: Evaluation with the presence of tampering attack in IDRM

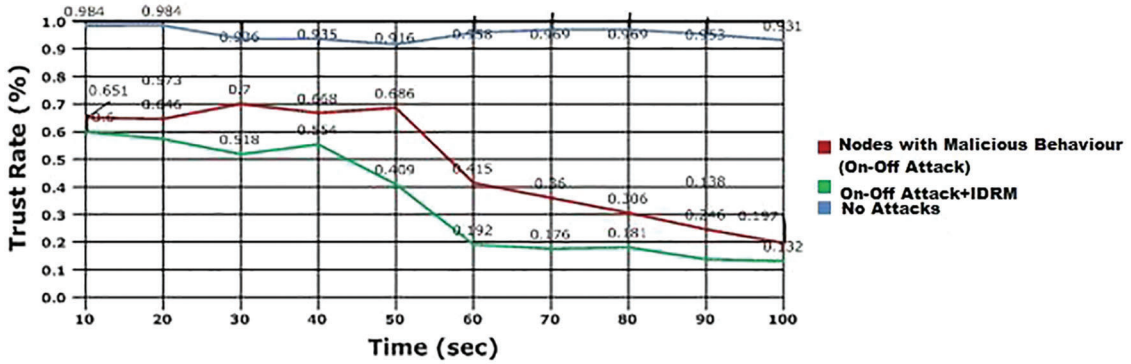

Figure 7: Analysis with On-Off attacks in IDRM

In Fig. 6, it is explicit that the average PDR obtained by the proposed model IDRM, even in the presence of tampering attacks is considerably higher. Initially, when it is considered that no attacks in the model, the PDR will be higher with seamless transmission of packets. But, when the tampering attacks affect the network, the delivery rate is reduced the proposed Improved Defensive Routing Mechanism has the delivery rate of packet is considerably improved. The main function of the proposed model is to derive the trust rate of the sensor nodes and the path between nodes. The results are presented in Fig. 7 with the consideration of On-Off Attacks in the network. The trust rate at the presence of attacks is lower for the nodes; hence, those nodes are not being given importance in secure route framing mechanism of the adduced work.

Routing Overhead is another important factor for analysing the performance of the proposed routing model. The comparative results on routing overhead are presented in the Fig. 8. In Fig. 9 evaluation results on transmission delay are depicted. Because of effective trust rate evaluations and secure routing functions, the proposed model provides minimal routing overhead and delay compared to SAR and TSR.

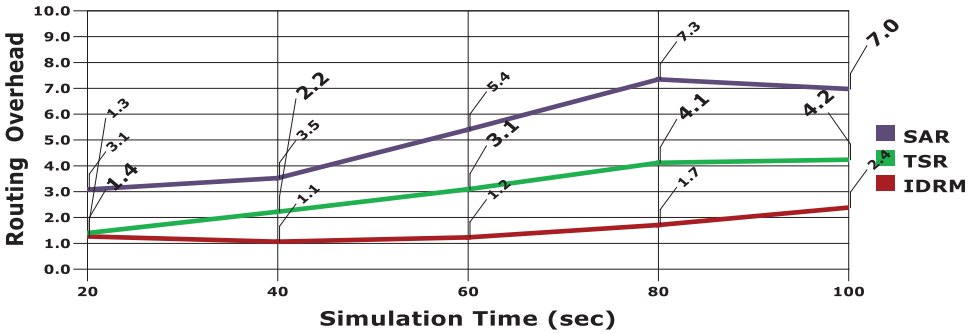

Figure 8: Routing overhead comparison

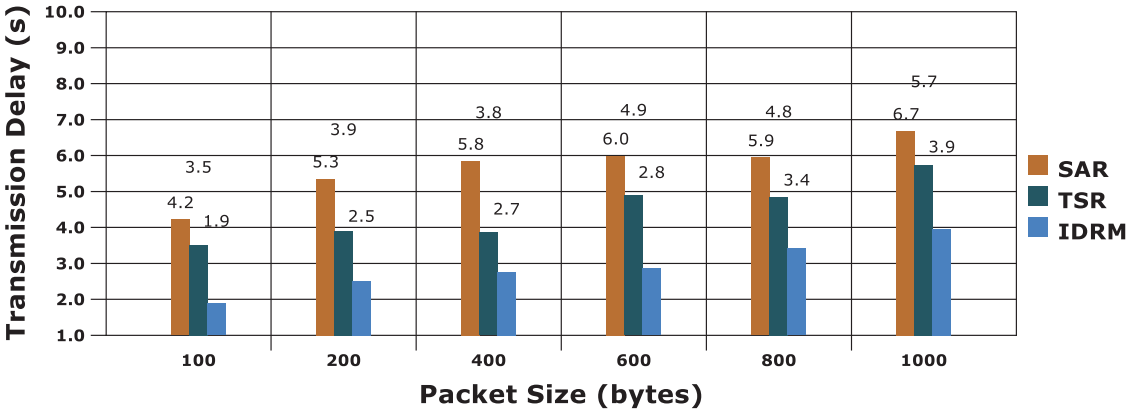

Figure 9: Transmission delay evaluations

In Fig. 10 the presence of malicious nodes packet drop rate will be higher. The effective incorporation of the defensive model, in the proposed system results in minimal packet drop, which is about 38% than the existing models. Another significant factor in performance evaluation is throughput, which determines the effective packet delivery of the communication model in WSN. The obtained results are portrayed in Fig. 11. It is observed from the figure that the proposed IDRM produces higher throughput value and the value accounts to an average of 91.4%.

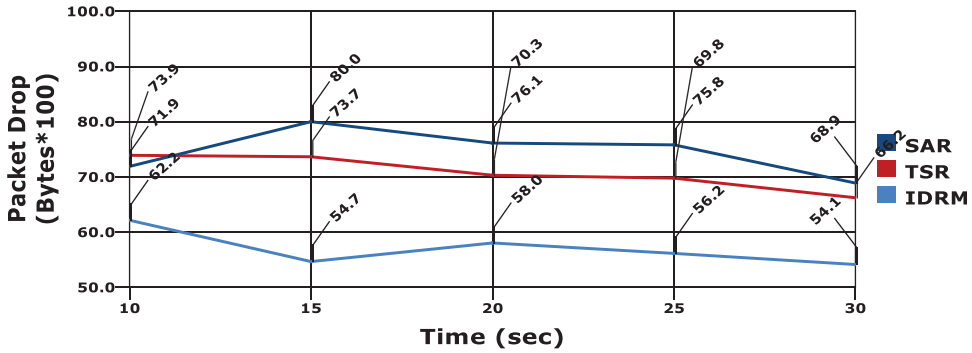

Figure 10: Packet drop evaluation between models

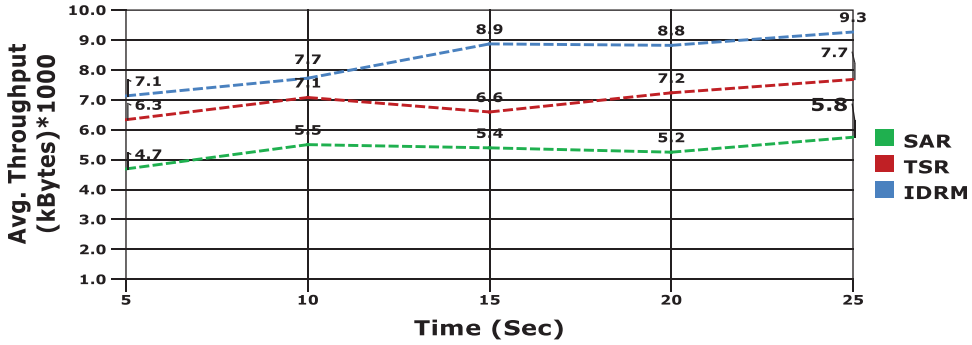

Figure 11: Results of throughput evaluation between models

6 Conclusion and Future Work

This paper develops a novel security model for secure packet transmission in heterogeneous wireless sensor networks. The proposed IDRM, includes node security evaluation and computation for secure paths. Additionally optimal secure routes are framed based on the trust rate computations for data forwarding. While framing the optimal secure routing using IDRM, trust parameters and QoS parameters are also considered. Moreover, the performance of the proposed model is evaluated based on the metrics such as transmission delay, packet delivery ratio, routing overhead, throughput and so on. The results prove that the model outperforms the existing models and is highly efficient when evaluated based on some common security attacks.

In future, the work can be enhanced by defining more accurate secure model in wireless sensor network and IoT based functions can also be included.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Watteyne and K. S. J. Pister, "Smarter cities through standards-based wireless sensor networks," *IBMJournal of Research and Development*, vol. 55, no. 1–2, pp. 7–10, 2011.

[2] B. C. Villaverde, S. Rea and D. Pesch, "InRouta QoS aware route selection algorithm for industrial wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 458–478, 2012.

[3] Y. Cao, C. Xu, J. Guan, F. Song and H. Zhang, "Environment-aware CMT for efficient video delivery in wireless multimedia sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, no. 11, pp. 381726, 2012.

[4] D. A. Tran and H. Raghavendra, "Congestion adaptive routing in mobile ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 11, pp. 1294–1305, 2006.

[5] L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile Ad hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[6] C. Zhang, X. Zhu, Y. Song and Y. Fang, "A formal study of trust based routing in wireless ad hoc networks," in *Proc. of the IEEE INFOCOM*, San Diego, CA, USA, 2010.

[7] D. Djenouri, L. Khelladi and N. Badache, "A survey of security issues in mobile ad hoc networks," *IEEE Communications Surveys*, vol. 7, no. 4, pp. 2–28, 2005.

[8] Y. Zhou, Y. Fang and Y. Zhang, "Securing wireless sensor networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[9] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: Fairness in dynamic ad-hoc networks)," in *Proc. of the 3rd ACM Int. Symp. on Mobile Ad Hoc Networking and Computing (MOBIHOC '02)*, Lausanne Switzerland, pp. 226–236, 2002.

[10] S. Paris, C. Nita-Rotaru, F. Martignon and A. Capone, "EFW: A cross-layer metric for reliable routing in wireless mesh networks with selfish participants," in *Proc. of the IEEE INFOCOM*, Shanghai, China, pp. 576–580, 2011.

[11] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[12] P. Ning, A. Liu and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 1, pp. 1–35, 2008.

[13] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[14] S. Archana and A. Saravana Salvan, "SAR protocol based secure data aggregation in Wireless Sensor Network," in *IEEE 9th Int. Conf. on Intelligent Systems and Control (ISCO)*, Coimbatore, India, pp. 1–6, 2015.

[15] P. Narula, S. K. Dhurandher, S. Misra and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing," *Computer Communications*, vol. 31, no. 4, pp. 760–769, 2008.

[16] M. E. Mahmoud and X. Shen, "Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks," in *Proc. of the IEEE Int. Conf. on Communications (ICC '11)*, Kyoto, Japan, 2011.

[17] K. S. Hung, K.-S. Lui and Y.-K. Kwok, "A trust-based geographical routing scheme in sensor networks," in *Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC '07)*, Hong Kong, China, pp. 3125–3129, 2007.

[18] T. Yang, X. Xiangyang, L. Peng, L. Tonghui and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia Computer Science*, vol. 131, no. 4, pp. 1156–1163, 2018.

[19] M. Mohi, A. Movaghar and P. M. Zadeh, "A Bayesian game approach for preventing DoS attacks in wireless sensor networks," in *Proc. of the IEEE Int. Conf. on Communications and Mobile Computing (CMC'09)*, Kunming, China, pp. 507–511, 2009.

[20] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, 2003.

[21] Y. Yu, K. Li, W. Zhou and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[22] F. Ishmanov and Y. Bin Zikria, "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues," *Journal of Sensors*, vol. 2017, pp. 1–16, 2017.

[23] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[24] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng *et al.,* "Highly reliable trust establishment scheme in ad hoc networks," *Computer Networks*, vol. 45, no. 6, pp. 687–699, 2004.

[25] H. Xia, Z. Jia, X. Li, L. Ju and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Networks*, vol. 11, no. 7, pp. 2096–2114, 2013.

[26] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless Personal Communications*, vol. 69, no. 2, pp. 805–826, 2013.

[27] R. Dhanapal and P. Visalakshi, "Optimizing trust based secure routing for unified efficient resource sharing for large scale MANET-TSRRS," *Asian Journal of Information Technology*, vol. 15, no. 19, pp. 3756–3762, 2016.

[28] R. Saranyadevi, M. Shobana and S. Karthik, "A survey on preventing jamming attack in wireless communication," *International Journal of Computer Applications*, vol. 57, no. 23, pp. 1–3, 2012.

[29] M. Shobana, R. Saranyadevi and S. Karthik, "Geographic routing used in manet for black hole detection," in *Proc. of the Second Int. Conf. on Computational Science, Engineering and Information Technology*, ACM Digital Library, Coimbatore, India, pp. 201–204, 2012.

[30] S. Awan, M. Bint, E. Sajid, S. Amjad, U. Aziz *et al.,* "Blockchain based authentication and trust evaluation mechanism for secure routing in wireless sensor networks," in *Int. Conf. on Innovative Mobile and Internet Service in Ubiquitous Computing*, Asan, Korea (Republic of), vol. 279, pp. 96–107, 2021.

[31] S. Huang, A. Liu, S. Zhang, T. Wang and Neal N. Xiong, "N BD-VTE: A novel baseline data based verifiable trust evaluation scheme for smart network systems," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2087–2105, 2021.

[32] N. Satheesh Kumar, V. Kavitha, T. Menaka and V. Manonmani, "Selfish node avoidance using adaptive trust computation model in WSN," *European Journal of Clinical and Molecular Medicine*, vol. 7, no. 11, pp. 2454–2461, 2020.

[33] Jeelani, Kishan Pal Singh and Aasim Zafar, "A trust calculation algorithm for communicating nodes in Wireless Sensor Networks," *International Research Journal on Advanced Science Hub*, vol. 3, no. 3, pp. 145–152, 2021.

[34] Y. L. Sun, Z. Han, W. Yu and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proc. of the 25th IEEE Int. Conf. on Computer Communications (INFOCOM '06)*, Barcelona, Spain, pp. 1–13, 2006.