Wireless Personal Communications (2019) 105:1475–1490
https://doi.org/10.1007/s11277-019-06155-x

An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks

M. Selvi[1] · K. Thangaramya[1] · Sannasi Ganapathy[2] · K. Kulothungan[1] · H. Khannah Nehemiah[1] · A. Kannan[1]

Published online: 13 February 2019

Abstract
Security is an important phenomena for energy conservation in wireless sensor networks (WSN). Moreover, the management of trust in the WSN is a challenging task since trust is used when collaboration is critical to achieve reliable communication. In a military application using WSN, it is often necessary to communicate secret information such as military operation urgently. However, the existing routing algorithms do not consider security in the routing process. Moreover, since security is an important aspect in WSN, it is necessary to consider the security aspects in routing algorithms. Different approaches for providing security are trust management, intrusion detection, firewalls and key management are considered in the literature. Among them, trust management can provide enhanced security when it is compared with other security methods. Therefore, a new secure routing algorithm called energy aware trust based secure routing algorithm is proposed in this paper where the trust score evaluation is used to detect the malicious users effectively in WSN and spatio-temporal constraints are used with decision tree algorithm for selecting the best route. From the experiments conducted, it is proved that the proposed trust based routing algorithm achieves significant performance improvement over the existing schemes in terms of security, energy efficiency and packet delivery ratio.

Keywords Intrusion detection · Wireless sensor networks · Trust score · Secure routing · Malicious nodes · EATSRA

1 Introduction

Wireless sensor networks (WSNs) provide wireless services by sensing the environment. In WSN, power consumption is a main challenge and in addition security is also a major concern. Hence, many researchers are working in this field to reduce the energy utilization with the help of the routing protocol. WSNs are categorized into structured and unstructured types of networks. The collection of dense sensor nodes deployed in an ad-hoc nature

✉ M. Selvi
arpudhaselvi123@gmail.com

Extended author information available on the last page of the article

is called as unstructured WSN. On the other hand, when all nodes are deployed based on a preplanned manner then the network is called as structured WSN.

Recently, WSN become an insecure environment due to the vulnerable attacks which are performed on several nodes by attackers. Some of the attacks which are carried out at the routing level are called black hole, Sybil, spoofing and denial of service (DoS) attacks. Among them, DoS attack is the most important security challenge. Therefore, many researchers are working for developing a new secure routing protocol to secure the WSN. A new energy efficient routing algorithm is proposed in this work which saves energy by identifying and preventing security attacks. The energy consumption problem in WSN occurs when nodes involve in malicious activities. Therefore, we identified that the energy of sensor nodes can be saved by preventing the malicious activities.

In order to provide secure communication, it is necessary to provide a secured path in such a way that the proposed path will be identified by computing the trust which identifies the genuineness of the participating nodes. The trust is defined as a level of confidence of neighborhood nodes to send and receive packet securely while performing routing. In this work, a new trust based secure routing protocol called energy aware trust based secure routing algorithm (EATSRA) is proposed in which the trust metrics are used to address the security issues based on our protocol by monitoring node behavior, packet delivery ratio, received signal strength and residual energy. This approach improves efficiency and reduces energy consumption by identifying and avoiding the malicious node attacks. In order to prevent the security issues in WSN, evaluating trust between the neighborhood nodes is must. Trust values are evaluated based on direct and indirect trust or recommendation trust values [1]. The both successful and unsuccessful interaction between neighbor nodes is called as direct trust. Recommending one node to another node is called as recommendation trust or indirect trust. According to the trust values the effective and efficient communication between the nodes are carried out and the decisions are made to select the best path to reach the destination but the trust on particular node varies with time and the trust values also increases or decreases with time. The communication is performed only through the genuine nodes which are identified by calculating the trust. The particular attacks are identified by using the total trust of the nodes which is obtained from direct trust and indirect trust.

Many routing protocols are used for effective communications that are only useful for transmitting the data from one node to another node with lower energy. The protocols used for effective communication should only provide either energy efficient routing or trust based routing. Therefore, a new secure routing algorithm called EATSRA has been proposed in this paper. Moreover, a new trust score evaluation model is proposed in this work to detect the malicious users effectively in WSN and spatio-temporal constraints are used with decision tree algorithm for selecting the best route. However, the proposed routing protocol provides a better solution for providing effective communication with the help of energy efficient trust based routing technique. Moreover, trust is used in this work for identifying malicious nodes which enables secure routing. Therefore, this paper proposes a new decision tree and trust based security mechanism that identifies the intruders using the trust scores and provides better network performance in terms of throughput, packet delivery ratio and reduced delay. The main advantage of this trust based security model is that the malicious nodes can be easily identified and avoided.

The remainder of this paper is organized as follows: Sect. 2 provides a survey of related works in the areas of cluster based routing and secure routing algorithms. Section 3 explains the proposed work and the algorithms proposed in this paper for performing the secure routing process. Section 4 presents the results obtained from this work and they are compared with the existing work. Section 5 gives conclusion on this work and suggests some suitable future work.

2 Literature Survey

Wireless Sensors are applied in various fields [2–6] which include health monitoring, defense control, agriculture precision, monitoring gasoline pipelines, temperature sensing and underground mining [7]. Routing is a key challenge in wireless sensor network [8] and it tends to make an error due to some reasons which includes limited battery power, behavior of malicious nodes, continuous node failures and changing network conditions. Al-Karaki et al. [9], classified the routing protocols with respect to the structure of the network namely flat, hierarchical and location based routings. In flat-based routing all nodes are treated equally and the data are forwarded from one node to another node until the data reaches the sink. In hierarchical-based routing all nodes are not treated equally because in this routing protocol one sensor node is considered as a cluster head which was chosen among the sensors which are presented in a cluster. Therefore, in this protocol all information's are routed through cluster head to the sink node. Here, the location information is taken into an account to make a proper routing and also it is considered as context aware routing. Probably these kinds of protocols are applied in military and ubiquitous learning applications. Ian et al. [10] discussed about routing challenges in wireless sensor networks which are energy consumption while discovering the neighbor nodes and communicating to each other. The other challenges are scalability, addressing, robustness, topology and different routing techniques needed for different applications. Utilizing energy in an efficient manner is a key challenge in wireless sensor network. Energy depletion occurs not only for transmission and reception purpose, but also for sensing the idle channel [7].

Kesavan et al. [11] proposed a dynamic keying approach for securing the communication system with the help of effective clustering techniques to validate the nodes during mobility. In this approach, keys are generated dynamically and are provides secure communication over the network. If the previously used keys are stolen by attackers the same key cannot be reused by intruders to compromise the network. Trusting a node is an important criterion while providing secure communication. The word trust is derived from the study of social science. Recently the researchers are moving forward to apply this trust concept in social networking websites such as Facebook, Twitter, LinkedIn etc., Trust provides a reliable communication. In [12], authors explained about extension to LEACH protocol which was proposed by Heinzelman et al. [13] and it is of self-organizing and adaptive in nature with respect to cluster formation. This LEACH protocol uses a randomization technique for distributing the available energy in the sensor nodes for communication by changing the cluster heads through rotation among the sensors nodes presented in the network. Moreover, it performs the randomized rotation of the cluster heads among the sensor nodes mainly based on the distance of the node in order to enhance the performance. This is also useful to reduce the battery power usage in the sensors. Therefore, this feature provides an effective facility for making the nodes to perform balanced energy consumption during communication and hence it leads to a longer lifetime for the nodes presented in the network. This protocol separates the sensor networks' communication process into two main phases namely the set up phase and the steady state phase. In the first phase called set-up phase, each cluster member in the network decides whether to become a cluster head for the current cluster in this round. For this purpose, the existing cluster head broadcasts an advertisement message to all the member nodes of the cluster. Moreover, the respective cluster heads are selected in this protocol depending on the signal strength of the advertisement message. Therefore, the cluster head creates a channel allocation scheme by applying the time division multiple access method and it assigns a time slot to each cluster

member. In the next phase called the steady state phase, the cluster head nodes are collecting the data from the cluster members and they combine them to form a consolidated data which are sent to the sink node. In this model, the sensor nodes are location unaware and hence the hop count is used to measure the distance. Since all the above communication processes consume more energy, the energy must be conserved and used more efficiently. This is necessary because, since the battery of the nodes cannot be recharged and replaced. However, one limitation of LEACH protocol is that it does not consider the security issues and hence the energy consumed due to the presence of malicious nodes becomes a serious issue with respect to energy consumption. Therefore, this model proposed in this paper, enhances the LEACH protocol by considering energy and trust.

The HEED algorithm was proposed by Younis and Fahmy [14] in order to perform optimal and effective routing through the formation of cluster and by routing the packets through the cluster heads. The HEED protocol performs the cluster head selection by applying the effective probability values and following a random policy. Through these methods, packets are routed through the cluster heads and when the energy drains in the cluster head nodes, the cluster heads are changed through the application of the cluster head selection policies. This protocol provides equal chance to all the nodes for becoming the cluster heads. Therefore, it provides better routing performance by the formation of small clusters. The major limitation of this protocol is its dependency on the energy parameters rather than considering the other quality of service metrics. Many authors have attempted to model trust in mathematical way. One of the work proposed based on information theoretic model based trust evaluation [15], where uncertainty was modeled effectively using higher order logics such as fuzzy logic, temporal logic and modal logic. All these logics help to predict the future behavior using past data and constraints. Das et al. [16] presented a novel trust computation model called secured trust based routing model (STRM) for secure routing in order to evaluate the available agents in multi-agent environments. The main advantage of this protocol is that it performs routing through agents and hence provides better coordination in the communication. However, this protocol has the limitation of routing overheads by involving more nodes in the communication process. Li et al. [17] proposed a certainty oriented reputation system for network security. Mohammed et al. [18] explained the methods for detection of selfish and malicious nodes in wireless environment. Li et al. [19] proposed a metric to compute path trust to develop a secure routing algorithm. Wang et al. [20] designed a routing protocol based on trust for optimal routing in WSN. Yan et al. [21] proposed a system for trust management for developing a component based system where the trust is calculated dynamically. Wang et al. [1] introduce a new model for trust aggregation based on Markov model linearly. It also supports the trust aggregation for calculate the average trust of the network. Serique et al. [22] proposed trust evaluation mechanism to develop a secure routing protocol. Wang et al. [23] proposed a novel two-dimensional aggregation model for trust management. Xia et al. [5] introduced a new trust model for secure routing process in mobile ad hoc networks. There are many works in routing that use spatial [24] and temporal constraints for making effective routing decisions [25].

In spite of the presence of many routing algorithms in the literature the security challenges are not considered in most of the existing protocols. Therefore, a new energy efficient trust based routing protocol which uses decision tree algorithm for making effective decisions with respect to routing is proposed in this paper. The main advantage of the propose algorithm is increase in security and performance with less energy consumption.

3 Proposed System

The proposed algorithm consists of four phases namely trust score evaluation, threshold setting, Finding malicious nodes by using trust metrics and the EATSRA

3.1 Background Works for the Proposed System

The proposed model was developed based on the LEACH protocol and by adding the trust modeling for enhancing the security. Moreover, the results obtained from this work have been compared with the cluster based routing protocols namely LEACH and HEED and also it is compared with the trust based routing protocol STRM. The LEACH protocol was proposed by Heinzelman et al. [26] and it is of self-organizing and adaptive in nature with respect to cluster formation. This protocol uses a randomization technique for distributing the available energy in the sensor nodes for communication by changing the cluster heads through rotation among the sensors nodes presented in the network. Moreover, it performs the randomized rotation of the cluster heads among the sensor nodes mainly based on the distance of the node in order to enhance the performance. This is also useful to reduce the battery power usage in the sensors. Therefore, this feature provides an effective facility for making the nodes to perform balanced energy consumption during communication and hence it leads to a longer lifetime for the nodes presented in the network.

The LEACH protocol separates the sensor networks' communication process into two main phases namely the set up phase and the steady state phase. In the first phase called set-up phase, each cluster member in the network decides whether to become a cluster head for the current cluster in this round. For this purpose, the existing cluster head broadcasts an advertisement message to all the member nodes of the cluster. Moreover, the respective cluster heads are selected in this protocol depending on the signal strength of the advertisement message. Therefore, the cluster head creates a channel allocation scheme by applying the time division multiple access method and it assigns a time slot to each cluster member. In the next phase called the steady state phase, the cluster head nodes are collecting the data from the cluster members and they combine them to form a consolidated data which are sent to the sink node. In this model, the sensor nodes are location unaware and hence the hop count is used to measure the distance. Since all the above communication processes consume more energy, the energy must be conserved and used more efficiently. This is necessary because, since the battery of the nodes cannot be recharged and replaced. However, one limitation of LEACH protocol is that it does not consider the security issues and hence the energy consumed due to the presence of malicious nodes becomes a serious issue with respect to energy consumption. Therefore, this model proposed in this paper, enhances the LEACH protocol by considering energy and trust.

The HEED algorithm was proposed by Younis and Fahmy [14] which is a cluster based routing protocol for performing optimal routing in WSNs. This protocol selects the cluster heads through the use of probability values and by following a random method and such cluster heads are used to perform the cluster head based routing process. However, it tries to improve the efficiency by changing the cluster heads frequently and more uniformly across the sensor network through multiple iterations based on energy requirement and to provide smaller cluster ranges. Moreover, each member node in this model can also become a cluster head node using its own probability value due to the cluster head rotation policy and it is initiated by hearing no cluster head declaration message from the neighbor nodes. The major advantages of this protocol include the energy efficiency through cluster based routing and the

change of cluster head through a rotation policy to enhance the network lifetime. One of the limitations of this protocol is the use of random probability values for cluster head election.

In WSNs, security and privacy have become the major design issues and it is enforced using access control techniques, effective key management schemes and the use of intelligent agents. An agent system can be either a single user system or a multi-agent system. In the recent years, most network applications including pervasive computing systems, grid computing models and P2P networks use multiple agents and hence they are multi-agent systems that provide open, anonymous and dynamic type of secured communication. The characteristics of multi-agent systems are compromised by attackers due to the presence of weaker agents. Therefore, trust modeling and reputation modeling techniques are used in the secure routing protocol called secured trust based routing model (STRM). This system minimizes the threats by evaluating the trust and reputation of all the interacting agents present in the nodes. The main advantage of the STRM model is the provision of a dynamic trust model which identifies the malicious behavior based on workloads and isolates them. In this model, the authors first analyze the different characteristics related to the evaluation of the trust of an intelligent agent and then they proposed a new comprehensive quantitative model in order to measure the trust values called the first trust and second trust. Based on the trust modeling, the authors performed load balancing and network for enhancing the performance of distributed processing. One of the limitations of this protocol is the use of malicious agents also in the communication.

3.2 Trust Score Evaluation

In order to evaluate the trust of nodes, created the wireless scenario with 15 nodes and initially considered the trust values 0. The LEACH routing protocol is used for transmission in our topology [13]. We calculated the trust score for individual node based on the following two constraints. First, Nodes which genuinely sending their acknowledgement to neighbors whenever they received the packets are treated as first group. Second, nodes which dropped more packets are considered as group 2 nodes. Now initial trust score is computed using the Eq. (1) that represents the rate of genuine acknowledge.

$$TS_{(1,i)} = \frac{\left[W1 * \left(\frac{ACK}{RP} * 100\right) + W2 * Temp_{Score} + W3 * Spatial_{Score}\right]}{[\mathrm{W1} + \mathrm{W2} + \mathrm{W3}]} \tag{1}$$

where W1, W2 and W3 are the weights given to the different trust scores, $TS_{(1,i)}$ denote the first trust score in percentage for ith node, ACK represent the number of acknowledgements sent to the neighbors and RP indicates the number of packets received from neighbors.

The second trust score is computed using Eq. (2) which calculates the dropped packets.

$$TS_{(2,i)} = 100 - \left(\left(\frac{DP}{TDP}\right) * 100\right), \quad t1 < t \leq t2 \tag{2}$$

where $TS_{(2,i)}$ represents the second trust score in percentage for ith node, DP indicates the number of packets dropped and TDP indicates the total number of packets dropped in network and t is the temporal constraint to check the time boundaries t1 and t2 for lower and upper limits of the time interval.

Finally, we calculate the overall trust score of the particular node i by using the Eq. (3).

$$TS_i = \frac{\left(TS_{(1,i)} + TS_{(2,i)}\right)}{2} + \text{Recommendation Score} \tag{3}$$

where TS_i indicates the overall trust score for node i, $TS_{(1,i)}$ represents the first trust score for node I and $TS_{(2,i)}$ indicates the second trust score for node i.

3.3 Threshold

The signal strength of the node reduces with distance d. The Eq. (4) is adopted from [13, 27] to calculate the energy used to send k bits based on the distance between one node to another node.

$$E_{tx}(k,d) = k * E_{elec} + k * \varepsilon * d^n \tag{4}$$

where E_{tx} represents the energy used, E_{elec} represents the transmitting circuit loss. n takes the value of 2 or 4 depending upon free space or multipath fading. ε is the energy required by power amplification.

In LEACH protocol [13], cluster heads are elected based on Eq. 5. It shows the threshold value $T(k)$ with this value the cluster head is selected for m round with minimal amount of energy.

$$\mathrm{T(k)} = \frac{\mathrm{p}}{\{1 - \mathrm{p}^*(\mathrm{m}^*\mathrm{mod}(1/\mathrm{p}))\}} \tag{5}$$

where m is current round number and p is the desired percentage of cluster head.

In this work, we assign threshold based on the mean value of the overall trust score for all the nodes which is present in the network scenario. First, find the mean value using the overall trust scores by applying the Eq. 6 in this work.

$$TM = \sum_{i=1}^{n} TSi/_n \tag{6}$$

where TM means that the trust score mean value, *TSi* indicates the trust scores summation and n represents the number of nodes. TM is a threshold to find the malicious node from the network scenario.

3.4 Finding Malicious Nodes by Using Trust Metrics

The attacks which are addressed in this paper are identified and detected through packet delivery ratio (PDR), node behavior and residual energy.

3.4.1 Packet Delivery Ratio $\alpha^{B}_{A(t_1,t_2)}$

Packet delivery ratio $\alpha^{B}_{A(t_1,t_2)}$ at interval t1 and t2 is computed using Eq. (7).

$$\alpha^{B}_{A(t_1,t_2)} = \frac{\rho^{B}_{A(t_1,t_2)}}{\tau^{B}_{A(t_1,t_2)}} \tag{7}$$

$\rho^{B}_{A(t_1,t_2)}$ = Total number of packets delivered succesfully from node A to node B at time t_1 and t_2.

$\tau^{B}_{A(t_1,t_2)}$ = Total number of packets transmitted from node A to node B at time t_1 and t_2.

DoS attack can easily be detected by tracking the packet delivery ratio of nodes. The packet delivery ratio ranges between 0 and 1. In case of successful transmission of all the packets out of total number of transmitted packets, the PDR is 1. If the node does not transmit any number of packets successfully, the PDR is zero.

3.4.2 Node Behavior $\beta^{B}_{A(t_1,t_2)}$

The node behavior is computed using Eq. (8) in which ω_1 and ω_2 are used as the weights for trust score and mobility.

$$\beta^{B}_{A(t_1,t_2)} = \omega_1 * TSi^{A,B}_{(t_1,t_2)} + \omega_2 * Mobility \tag{8}$$

Since the locations of the nodes stay the same under static environments, it is possible to detect Sybil attack by just recording and comparing the ratio of RSSI for the received messages. They showed through experimentations that RSSI ratio values fluctuate a lot even for fixed nodes. To overcome the influence of RSSI ratio variation on inferring, a threshold is used to tolerate the difference of RSSI ratios. The threshold is defined as the five times of standard deviation of the RSSI ratios. Moreover, a random way mobility model is used for the simulation in this work. In order to mention this, the mobility parameter and the mobility model details are included in the simulation parameters.

3.4.3 Residual Energy $\gamma_{(t_1,t_2)}$

The residual energy is the energy available after performing a number of transmission activities. Since it is the remaining energy, it is used to find the new cluster head and to perform cluster head based routing. The residual energy is computed using Eq. (9).

$$\gamma_{(t_1,t_2)} = E_0 - \left(\left(T_{(t_1,t_2)} * E_{tx}\right) + \left(R_{(t_1,t_2)} * E_{rx}\right)\right) \tag{9}$$

where γ is the residual energy, E_0 is the initial energy, T is the trust value, E is the energy consumed value and R is the transmission range.

3.4.4 Normalization of Trust Parameters N

The trust parameters (α, β, γ) are normalized for making the computation effective. The values of all trust parameters are normalized between 0 and 1 by applying following Eq. (10).

$$N = \frac{\alpha^{B}_{A(t_1,t_2)} + \beta^{B}_{A(t_1,t_2)} + \gamma_{(t_1,t_2)}}{3} \tag{10}$$

3.5 Energy Aware Trust Based Secure Routing Algorithm

This algorithm contains two phases namely trust based secure routing and decision Tree based best path selection. In first phase, the proposed algorithm finds the secure path based on trust score. In second phase, the decision tree algorithm called Enhanced C4.5 [28] used for finding the best secure path from the selected paths. The steps of the proposed energy aware trust algorithm (EATSRA) are as follows:

Algorithm: *Energy Aware Trust based Secure Routing Algorithm*
Input: Collected Sensor Data
Output: Packet delivery and report on network performance
Phase 1: Trust based Secure Routing

Step 1: Initially, assign trust values as 0 for all nodes.

Step 2: Compute packet delivery ratio $\alpha^{B}_{A(t_1,t_2)}$ for each node.

Step 3: Set the time interval as $[t_1, t_2]$.

Step 4: Source node broadcast the route request packets to all its neighboring nodes.

Step 5: Neighboring node receives the request then it will check whether it is destination or not. If it is destination then it sends the acknowledgement to its neighboring nodes.

Step 6: Calculate the first trust score for all the nodes using $TS_{(1,i)} = \frac{\left[W1*\left(\frac{\Delta CK}{RP}*100\right)+W2*Temp_{Score}+W3*Spatial_{Score}\right]}{[\mathrm{W1+W2+W3}]}$.

Step 7: Calculate the second trust score for all the nodes using $TS_{(2,i)} = 100-\left(\left(\frac{DP}{TDP}\right)*100\right), \quad t1 < t \leq t2.$

Step 8: Calculate the overall trust score for all the nodes $TS_i = \frac{(TS_{(1,i)}+TS_{(2,i)})}{2}$.

Step 9: Calculate the threshold value for the network scenario using $TM = \sum_{i=1}^{n} TSi/_n$.

Step 10: To find the malicious nodes by using the following conditions.
If trust score > threshold, and normalized value N > 0.8 during $[t_1, t_2]$ then the node is normal in $[t_1, t_2]$.
If trust score $TSi < TM_i$, then the node is malicious or abnormal.

Step 11: Finally, detect all the malicious nodes from the network scenario and isolate malicious nodes $M_1, M_2, \ldots M_K$..

Phase 2: Decision Tree based Best Secured Path Selection

Step 1: Call the decision tree algorithm [28] for selecting the best secured path.

Step 2: Apply spatio temporal constraints to validate the best path.

Step 3: Find the trustful nodes in the secured path and call them $T_1, T_2, \ldots T_n$.

Step 4: Route the packets through trustful nodes $T_1, T_2, \ldots T_n$. to reach the destination.

Step 5: End session.

Table 1 Simulation parameters

Parameter	Value
Area (m^2)	200 m × 200 m
No. of sensor nodes	50–300
Basic routing protocol	LEACH
Energy of nodes	2 J
Initial energy	0.5 J
Packet size	1024 bits
E_{elec}	50 nJ/bit
Mobility model	Random way mobility
Mobility speed	10 m/s to 50 m/s

Table 2 Performance comparison of the routing protocols

Methods	Number of packets sent	Number of packets received	Packet delivery rate (%)
LEACH	36,429	28,738	78.87
HEED	36,429	29,454	80.85
STRM	36,429	31,569	86.65
EATSRA	36,429	34,544	94.8

This algorithm is providing better performance than the existing routing protocols for WSNs due to many reasons. First, it performs cluster head selection using effective trust modeling. Second, it rotates the cluster head only among the trusted nodes. Third, it uses spatial and temporal constraints to analyze the node behavior. Fourth, it uses a good mobility model to measure the mobility so that it is possible to select a cluster head with low mobility. Finally, it selects the cluster head with high energy, high trust and low mobility leading to increase in packet delivery ratio and security but reduction in delay.

4 Results and Discussion

For simulating our proposed routing protocol, we used NS2 (Version 2.34.1). The simulation parameters are shown in Table 1. Moreover, a 200 × 200 m square area was used to carry out the simulation. Initially, all the nodes are assumed to have equal energy of 2 J. The nodes were allowed to move from 10 m/s speed to 50 m/s speed to perform the experiments. The basic routing protocol was LEACH. However, the experiments were carried out using HEED, STRM and the proposed EATSRA protocols. In this model, trust values were measured and the malicious nodes were identified by applying the trust model proposed in this paper. All the malicious nodes were avoided by preventing them from taking part in the routing process.

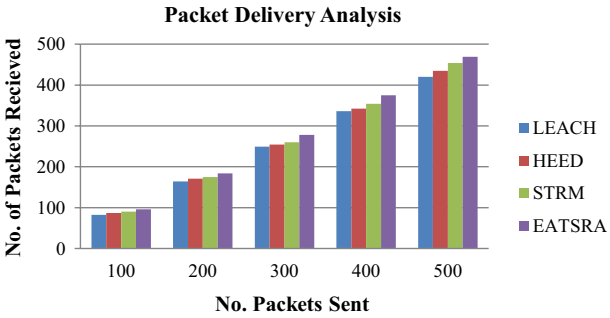
The LEACH routing protocol is used as the base protocol for carrying out all the simulations. Table 2 shows the performance comparison between LEACH, HEED, STRM and EATSRA by sending 36,429 packets in each experiment and they were tested with all the four protocols shown in Table 2.

From the Table 2, it can be observed that the overall performance is better for the proposed EATSRA when it is compared with LEACH, HEED and STRM. This is due to the use of trust management which identifies the malicious nodes and isolates them

Table 3 Delay analysis

Methods	Number of packets sent					
	6000	8000	10,000	12,000	14,000	16,000
Delay in LEACH (ms)	0.79	1.97	3.7	3.9	4.3	4.8
Delay in HEED (ms)	0.74	1.9	3.2	3.47	4.08	4.63
Delay in STRM (ms)	0.7	1.83	3.05	3.29	3.71	3.97
Delay in EATSRA (ms)	0.695	1.79	2.89	3.12	3.27	3.54

Fig. 1 Packet delivery analysis



from the routing process. Here, the security is increased leading to the increase in packet delivery rate. Moreover, the nodes were classified as genuine nodes and malicious nodes based on the trust scores using C 4.5 classification algorithm. Therefore, accurate decisions were made for isolating the malicious nodes from the routing process.

Table 3 shows the delay analysis comparison of LEACH, HEED and STRM protocol with the proposed EATSRA.

From Table 3, it is observed that the delay in the proposed routing protocol is less when compared to the LEACH, HEED and STRM protocols. The improvement is due to the provision of security in the proposed algorithm by implementing the proposed trust modeling. The recommendations made by the trust model have been considered in this work for allowing the nodes to send packets. Moreover, nodes with high trust, high energy and low mobility have been selected as the cluster head to enhance the reliability of communication.

Figure 1 shows the packet delivery rate analysis by considering the existing protocols namely LEACH, HEED, STRM and the proposed EATSRA. Here, the numbers of packets sent were varied from 100 packets to 500 packets in each of the experiments using all the four algorithms.

From Fig. 1, it can be observed that the packet delivery rate is gradually increasing in this proposed trust based routing protocol when it is compared with the existing LEACH, HEED and STRM protocols. This is due to the fact that the packets dropped by malicious nodes are avoided in this proposed work by applying the trust model proposed in this paper. Moreover, the cluster based routing technique considered only the nodes with high energy and trust to become the cluster head. This leads to reduction in packet drops and hence the packet delivery ratio is increased.

Figure 2 shows the energy consumption analysis between LEACH, HEED, STRM protocols and the proposed EATSRA. In this model, five experiments namely E1, E2, E3, E4

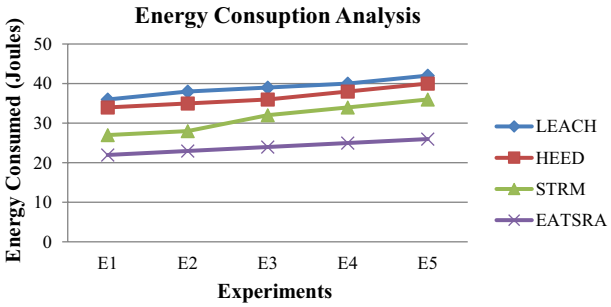


Fig. 2 Energy consumption analysis

and E5 were carried out by sending the collected packets from the nodes to the base station for a duration of 15 min each.

From Fig. 2, it can be observed that the energy consumption is less for the proposed EATSRA when it is compared with existing LEACH, HEED, STRM protocols. This is due to the fact that attacks are detected and malicious nodes are removed from the routing process. Moreover, the trust model used in this work considered spatial and temporal constraints to enhance the security restrictions. Therefore, the energy consumed by making flooding attacks by the malicious users is identified in advance and they are prevented. This leads to overall improvement in the network performance. This leads to reduction in energy consumption by the support of the proposed cluster based routing scheme.

Figure 3 shows the malicious node detection analysis between the proposed trust based routing protocol with spatio-temporal constraints and the existing routing protocols namely STRM and STRM with Decision tree classifier. In this model, the comparison is made between trust based routing protocols only since the security analysis is applicable more to these protocols.

From Fig. 3, it can be observed that the performance of the proposed routing protocol with respect to malicious node detection accuracy is better than the existing trust based protocols. This is due to the use of spatio-temporal features in the proposed trust based routing protocol. All the existing trust models assumed that the behaviors of nodes are same at all times and at any place. However in the proposed model, it is assumed that the behavior of nodes change with respect to time and location. Therefore, temporal and spatial constraints are used in the proposed model and hence more number of malicious

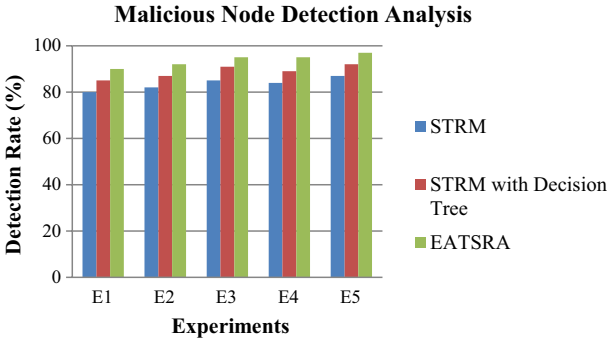


Fig. 3 Malicious node detection analysis

nodes are detected by the proposed model when it is compared with the existing trust based models.

5 Conclusion and Future Work

In this paper, a new secure routing algorithm called EATSRA is proposed and implemented for providing optimal and secure routing in WSN. In this model, the trust scores are used to detect the intruders more effectively in WSN and the decision tree based routing algorithm is used for selecting the best and secured path. Moreover, spatio-temporal constraints have been used for making routing decisions more effectively. From the experiments conducted using simulations, it is observed that the proposed EATSRA provides better performance by reducing the energy consumption and by enhancing the security as well as packet delivery ratio. Further works in this direction could be the use of intrusion detection facility as an additional feature using fuzzy constraints for handling incomplete knowledge more effectively.

References

1. Wang, X., Liu, L., & Jinshu, S. (2012). RLM: A general model for trust representation and aggregation. *IEEE Transactions on Services Computing, 5*(1), 131–143.
2. Jerusha, S., Kulothungan, K., & Kannan, A. (2012). Location aware cluster based routing in wireless sensor networks. *International Journal of Computer & Communication Technology, 3*(5), 1–6.
3. Kulothungan, K., Jothi, J. A. A., & Kannan, A. (2011). An adaptive fault tolerant routing protocol with error reporting scheme for wireless sensor networks. *European Journal of Scientific Research, 16*(1), 19–32.
4. Kulothungan, K., Ganapathy, S., Indra Gandhi, S., Yogesh, P., & Kannan, A. (2011). Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach. *International Journal of Soft Computing, 6*(5), 210–215.
5. Xia, H., Jia, Z., Ju, L., Li, X., & Sha, E. H.-M. (2013). Impact of trust model on on-demand multipath routing in mobile ad hoc networks. *Computer Communications, 36,* 1078–1093.
6. Selvi, M., & Nandhini, C., Thangaramya, K., Kulothungan, K., & Kannan, A. (2016). HBO based clustering and energy optimized routing algorithm for WSN. In *Proceedings of the eighth international conference on advanced computing (ICoAC)* (pp. 89–92).
7. Dargie, W., & Poellabauer, C. (2010). *Fundamentals of wireless sensor networks theory and practice*. Hoboken: Wiley. ISBN 978-0-470-99765-9.
8. Selvi, M., Logambigai, R., Ganapathy, S., Ramesh, L.S., Khanna Nehemiah, H., & Arputharaj, K. (2016). Fuzzy temporal approach for energy efficient routing in WSN. In *Proceedings of the international conference on informatics and analytics* (pp. 1–5). ACM.
9. Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications, 11,* 6–28.
10. Akyildiz, I. F., & Vuran, M. C. (2010). *Wireless sensor networks* (pp. 131–141). Hoboken: Wiley.
11. Kesavan, V. T., & Radhakrishnan, S. (2016). Cluster based secure dynamic keying technique for heterogeneous mobile wireless sensor networks. *China Communication, Security Schemes and Solutions, 13*(6), 178–194.
12. Ran, G., Zhang, H., & Gong, S. (2010). Improving on LEACH protocol of wireless sensor networks using fuzzy logic. *Journal of Information & Computational Science, 7*(3), 767–775.
13. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications, 1*(4), 660–670.
14. Younis, O., & Fahmy, S. (2004). HEED: A hybrid energy-efficient, distributed clustering approach for Ad Hoc sensor Networks. *IEEE Transaction on Mobile Computing, 3,* 366–379.

15. Sun, Y. L., Yu, W., Han, Z., & Liu, K. J. R. (2006). Information theoretic framework of trust modeling evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 305–319.
16. Das, A., & Islam, M. M. (2012). Secured trust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 261–274.
17. Li, F., & Wu, J. (2010). Uncertainty modeling and reduction in MANETs. *IEEE Transactions on Mobile Computing, 9*(7), 1035–1049.
18. Mohammed, N., Otrok, H., Wang, L., Debbabi, M., & Bhattacharya, P. (2011). Mechanism design-based secure leader election model for intrusion detection in MANET. *IEEE Transactions on Dependable and Secure Computing, 8*(1), 89–103.
19. Li, Z., Jia, P., Zhang, R., & Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Information Security, 4*(4), 212–232.
20. Wang, X., Ding, L., & Wang, S. (2011). Trust evaluation sensing for wireless sensor networks. *IEEE Transactions on Instrumentation and Measurement, 60*(6), 2088–2095.
21. Yan, Z., & Prehofer, C. (2011). Autonomic trust management for a component-based software system. *IEEE Transactions on Dependable and Secure Computing, 8*(6), 810–823.
22. Serique, L. F. S., & de Sousa, R. T. (2012). Evaluating trust in ad hoc network routing by induction of decision trees. *IEEE Latin America Transactions, 10*(1), 1332–1343.
23. Wang, Y., & Li, L. (2011). Two-dimensional trust rating aggregations in service-oriented applications. *IEEE Transactions on Services Computing, 4*(4), 257–271.
24. Mahmood, B. A., & Manivannan, D. (2015). Position based and hybrid routing protocols for mobile ad hoc networks: A survey. *Wireless Personal Communications, 83*(2), 1009–1033.
25. Manivannan, D., Jyotiprada, A., & Sandhu, N. (2014). A survey of routing protocols for wireless sensor networks. *International Journal of Next-Generation Computing, IJNGC, 5*(2), 1–8.
26. Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H. (2000). Energy-efficient communication protocol for wirelessmicrosensor networks. In *Proceedings of the 33rd annual Hawaii international conference on systemsciences, IEEE* (pp. 1–10).
27. Logambigai, R., & Kannan, A. (2016). Fuzzy logic based unequal clustering for wireless sensor networks. *Wireless Networks, 22,* 945–957.
28. Rajeswari, L. P., & Kannan, A. (2008). An intrusion detection system based on multiple level hybrid classifier using enhanced C4.5. In *IEEE international conference on signal processing, communications and networking* (pp. 75–79).

M. Selvi is currently pursuing Ph.D. in the Faculty of Information and Communication Engineering, Anna University Chennai in the area of Intelligent Energy Efficient Routing Algorithms for Wireless Sensor Networks. She has completed her M.E. from Anna University, Chennai in the year 2011. She has published 5 papers in journals and conferences. Her areas of interests are artificial intelligence, soft computing, and computer networks.

K. Thangaramya is currently pursuing Ph.D. in the Faculty of Information and Communication Engineering, Anna University Chennai in the area of Intelligent and Secure Routing Algorithms for Wireless Sensor Networks. She has completed her M.E. from Anna University, Chennai in the year 2014. She has published 2 papers in journals and conferences. Her areas of interest are artificial intelligence, soft computing, computer networks and security.

Sannasi Ganapathy is currently working as Assistant Professor (Sr. Gr) in VIT University, Chennai. He received his M.E. and Ph.D. degrees from Anna University, Chennai. He has published 50 articles in journals and conferences. His area of interest includes computer networks, soft computing, cloud computing and security.

K. Kulothungan is currently working as Assistant Professor (Sr. Gr) in the Department of Information Science and Technology, College of Engineering Guindy Campus, Anna University, Chennai. He received his M.E. and Ph.D. degrees from Sathyabama University and Anna University, Chennai respectively. He has published more than 40 articles in journals and conferences. His area of interest includes computer networks, soft computing, cloud computing and security.

H. Khannah Nehemiah is currently working as an Associate Professor in Ramanujan Computing Centre, Anna University, Chennai. He received his M.E. and Ph.D. degrees in Computer Science and Engineering from University of Madras and Anna University respectively. He has published more than 65 articles in journals and conference proceedings. His area of interest includes databases, artificial intelligence, networking and image processing.

A. Kannan is currently working as a Professor and Head in Anna University, Chennai where he received his M.E. and Ph.D. degrees in Computer Science and Engineering. He has published more than 300 articles in journals and conferences. His area of interest includes databases, artificial intelligence and security.

Affiliations

M. Selvi[1] · K. Thangaramya[1] · Sannasi Ganapathy[2] · K. Kulothungan[1] · H. Khannah Nehemiah[1] · A. Kannan[1]

K. Thangaramya
thangaramya112@gmail.com

Sannasi Ganapathy
sganapathy@vit.ac.in

K. Kulothungan
kulo@auist.net

H. Khannah Nehemiah
nehemiah@annauniv.edu

A. Kannan
kannan@annauniv.edu

[1] Department of Information Science and Technology, CEG Campus, Anna University, Chennai, India

[2] School of Computing Science and Engineering, VIT University, Chennai, India