International Journal of Information System Modeling and Design
Volume 8 • Issue 2 • April-June 2017

An Energy Efficient Trust Aware Opportunistic Routing Protocol for Wireless Sensor Network

Nagesh Kumar, Jaypee University of Information Technology, Waknaghat, India
Yashwant Singh, Central University of Jammu, Jammu, India
Pradeep Kumar Singh, Department of CSE and IT, Jaypee University of Information Technology, Waknaghat, India

ABSTRACT

As the wireless sensor networks (WSN) are gaining popularity the need of reliable delivery of data packets becomes more important. The reliable delivery is only possible when the routing protocols are efficient and secure. Because of lack of resources it is not possible to use existing cryptosystems to provide security in WSN. But, trust aware routing can provide the security with lesser resources, which become popular in last three to four years. In this paper, a new energy efficient and trust aware reliable opportunistic routing (TAEROR) protocol is proposed. The protocol consists of a trust metric and also a relay selection algorithm. The trust aware metric detects the malicious nodes on the basis of forwarding sincerity, energy consumption and acknowledgement sincerity. Relay selection algorithms avoid these malicious nodes to get selected in the routing process. The protocol is simulated and compared to existing trust aware routing protocols. Proposed protocol TEAROR presents better results than the other compared protocols.

KEYWORDS

Energy Efficiency, Opportunistic Routing, Sensor, Trust, WSN

1. INTRODUCTION

In most of the applications of Wireless Sensor Networks (WSN), the sensor nodes are operating independently without any external interference. This unsupervised operation of WSN leads to expose nodes to variety of malicious attacks. There are many protocols (Haque et al., 2008) (Hu et al., 2003) (Zhang et al., 2008) (Mohaisen et al., 2009) (Ahmed et al., 2016) developed, most of which are based on cryptographic and authentication systems. These algorithms/protocols are not successful for wireless sensor networks for the following reasons:

1. These protocols are mostly based on the assumption that all nodes in the network are helpful and truthful during the routing process. This assumption makes the protocols unrealistic especially for insider attacks (Slehi et al., 2016);

DOI: 10.4018/IJISMD.2017040102

2. The sensor nodes are having limited resources like battery power, storage capacity and processing capacity. These constraints restrict the use of the most of cryptographic algorithms. Because cryptosystems need to be executed with high processing, storage and power consumption (Ahmed et al., 2016);
3. In cryptographic and authentication systems there is requirement of centralized key management agent which is not possible to install in WSN.

For the purpose of security of data packets and routing processes in WSN trust and reputation based systems were proved to be more efficient against node mischievousness occurrences. Trust and reputation aware methods are new to solve the problem of security without using cryptosystems (Cordasco and Wetzel, 2008). The trust of a node in wireless communication networks can be defined as the "…degree of reliability of neighbor nodes performing routing process (sending and receiving packets) …" (Govindan and Mohapatra, 2012). These methods help the sensor nodes in making decisions about other nodes to select them as next-hop forwarders, in other words trust and reputation based routing methods predict the future behavior of neighbor nodes. As the WSN are opportunistic networks in nature, hence, trust and reputation based security systems are more suitable. In opportunistic networks every node on the routing path have the opportunity of send data toward the destination and no fixed path is followed. Hence, trust and reputation based methods helps the opportunistic routing processes to decide the best next-hop forwarder. Trust based methods in WSN are similar to the human behavior system, where two nodes will communicate to each other only when the trust level of receiving node is up to the mark at a certain period of time. The trust values of sensor nodes in WSN should be updated after a certain period of time for the purpose of maintaining low risk level. As the trust based routing protocols do not involve the malicious and misbehaving nodes into the routing process, the throughput and energy efficiency of the network will be improved automatically.

Working on trust and reputation based methods in recent years many protocols have been proposed (Srinivasan et al., 2006) (Ganeriwal et al., 2008) (Michiardi and Molva 2002) (Zaharia et al., 2013) (Tanachaiwiwat et al., 2004) (Gheorghe et al., 2013) (Choudhary et al., 2008) (Channa and Ahmed, 2011). However, most of the protocols have fixed path routing processes. In WSN the fixed path routing processes introduce delays and also if any node on the fixed path is dead, then routing processes are needed to rebuild it. Also, existing trust and reputation based approaches have many vulnerabilities. For example, most of the trusted nodes, in a trust based routing protocol, are the neighbor nodes which are having low energy. This will lead to a short network lifetime. There are several number of packets flow in the network at the same time, which increase the overhead of routing processes. Also, most of the trusted protocols are designed for MANETS and executed on strong hardware platforms having good resources. There is a need of dynamic trust based routing processes to detect the malicious behaviors in the network.

Opportunistic routing provides the ability to sensor nodes to utilize the broadcasting capabilities in a better way. Although there is a risk to data and routing process because of broadcasting, because when the node broadcast a packet it can also be received by malicious nodes. The malicious nodes can misuse these packets to destroy network or to spread false information. The motivation is to provide security to these packets as well as enhance the network lifetime by reducing the energy consumption. The trust aware protocols provide this facility with less energy consumption. The trusted nodes will be included in the routing process and the malicious or untrusted nodes will be avoided.

This paper announces a new trust based and reliable opportunistic routing protocol for WSN. The protocol has been designed to overcome the limitations of existing trust based routing schemes

discussed above. The proposed protocol introduces the direct trust evaluation for each 1-hop neighbor node. The trust evaluation is based on the forwarding sincerity, energy consumption and acknowledgement forwarding sincerity of 1-hop neighbor nodes. The protocols is opportunistic in nature and selects best next-hop always, when a node has the data to be transferred toward base station (destination). The proposed protocol is independent of node's location and it proves to be best in the presence of substantial network load. The proposed protocol always selects the best next hop, which is energy efficient and trustworthy. The simulation results depict the good performance of proposed protocol in the presence of hostile environment. It improves the network throughput, energy efficiency and end-to-end delays in the network.

In the rest of this paper the related work will be discussed in section 2. Section 3 provides the details about proposed protocol following with simulation results in section 4. Section 5 will discuss the conclusion and future perspective of the paper.

2. RELATED WORK

As far as opportunistic routing has been concerned there is a lot of work has been carried out by many authors (Kumar and Singh, 2017). But there is either no or very few trust or reputation aware secure opportunistic routing protocols proposed in past years (Slehi et al., 2016). Nowadays many researchers are focusing in this direction, because trust aware routing processes are lightweight and easy to implement in real applications. Opportunistic routing is mainly constituted of two phases, i.e. candidate set selection and forwarder selection out of that candidate set. (Liu et al., 2007), (Hsu et al., 2011) and (Darehshoorzadeh and Cedra-Alabern, 2012) published detailed reviews on OR notions, representations, and classifications.

The first and foremost opportunistic routing algorithm proposed was Ex-OR (Exclusive opportunistic routing) (Biswas and Morris, 2005). The algorithm worked well in the presence of wireless links. The algorithm was based on a routing metric known as expected transmission count (ETX), which is concerned with number of transmissions required for a packet to reach the destination. Working in same direction LCOR (Dubois-Ferriere et al., 2011) was proposed using the modified metric expected anypath transmission (EAX) (Zhong et al., 2006). SOAR (Rozner et al., 2009) also used the ETX and a mechanism to reduce number of duplicate packets sent towards the base station. Opportunistic routing was focused by many researchers, especially for WSN, by designing new routing protocols like POR (Liu et al., 2013), DPOR (Darehshoorzadeh and Cedra-Alabern, 2012) and CBF (Fubler et al., 2003), etc. All of these protocols do not consider security as a major parameter and apply no security method.

The packets in the sensor network transmitted through wireless channels and are exposed to attackers. Cryptosystems provide security from external attacks, but fails to cope up with internal malicious nodes in the network. For the purpose of securing network from internal attackers the cooperation among all sensor nodes is most important. To accomplish this task lightweight trust and reputation aware protocols are very important and these can provide security from internal as well as external attackers. Working in this direction many protocols have been proposed for wireless networks. Some common examples are CORE (Michiardi and Molva, 2002), SORI (He et al., 2004), CONFIDANT (Ganeriwal et al., 2008), PFM (mantas et al., 2017) and (Salehi et al., 2016) etc. All of these protocols are not primarily made for WSN, and hence do not work efficiently when used with WSN.

In WSN trust and reputation based systems has been focused by many researchers around the world in recent two or three years. The researchers tried to maintain the balance between the sensor resources and security of the network. A dynamic trust aware routing framework (TARF) has been proposed by (Deng et al., 2010). This framework utilizes the social network trust principles with traditional cryptographic models to secure the network. Another protocol efficient monitoring procedure in reputation system (EMPIRE) (Maarouf et al., 2009) was proposed for the purpose of probabilistic and

distributive monitoring methods. The authors tried to reduce the number of monitoring jobs for each node and hence reduce energy consumption in the network. Energy efficient and trust aware routing (ETARP) (Gong et al., 2015) is another protocol for WSN which ensures the maximum utilization of resources with minimum routing cost. Similarly, trust and energy aware secure routing protocol (TESRP) (Ahmed et al., 2016) reduces energy consumption and also lower the routing overhead in the network. Trust and location aware routing (TLAR) (Vamsi and Kant, 2016) is proposed recently and consider different parameters like forwarding sincerity, network acknowledgements, packet integrity, energy information, and feedbacks of other nodes. But the overhead and end-to-end delay increases when there is involvement of too many parameters.

From literature it is clear that trust management for WSN is being recognized only in last three to four years. Hence, there is not enough research work in the literature in terms of opportunistic routing techniques. Energy efficiency and link reliability has not been considered in most of the protocols. In this research work, a new trust aware routing protocol has been proposed and compared by using simulation with other existing protocols. The performance will be tested on the basis of simulations performed for various parameters.

3. PROPOSED PROTOCOL

In this section, proposed protocol will be discussed in detail. Before going into the details assumptions for the protocol are as follows:

1. The nodes are deployed randomly in the application area to be monitored;
2. The resources like energy, buffer size and computation power are fixed and same for every node;
3. A selfish or overloaded node will drop all the packets coming to it and also presents false energy and storage information;
4. Malicious nodes randomly drop some of the packets and lead to grey-hole attack. Some malicious nodes drop all of the packets and will lead to black hole attack.

3.1. Trust Aware Energy Efficient and Reliable Opportunistic Routing Protocol (TAEROR)

TAEROR is a dynamic routing protocol for wireless sensor networks. It is designed especially for WSN by considering the limited resources of each sensor node in the network. This protocol is based on opportunistic routing technique. In opportunistic routing forwarder candidate selection is the most important step. Hence, while designing an opportunistic routing algorithm a metric has to design, which helps the protocol to select good forwarder candidates.

The protocol TAEROR will be completed in multiple phases. In the starting stage of the network the neighbor nodes are identified and a neighbor list (NGH) is formed in each node. This will be completed by using hello packets, the nodes which are replying to the hello packets will be added to NGH. After forming neighbor lists, the trust-based opportunistic routing metric has been calculated and forwarder candidates will be selected. Energy cost model will be the same as in (Kumar and Singh, 2016). All of the phases will be discussed in the following subsections.

3.1.1. Trust Evaluation

This phase evaluates the trust value of a node and the next-hop relay will be selected on the basis of this trust value. The trust metric is based on the beta distribution and probability of a node being malicious. Only the direct trust values are taken into account in the proposed metric. Every time a when a node has data packets for transmission toward base station it initiates the opportunistic routing process. After forming the neighbor list, the trust value has been calculated for each node in the neighbor list. The trust value incorporates the probability of a node being malicious (P_m), forwarding sincerity (F),

acknowledgement sincerity (*ACK*) and energy depletion (*E*). The probability of a node being malicious is calculated on the basis of packets dropped during the routing process. It is calculated by using the unsuccessful packet forwarding ratio and the delay ratio for packet forwarding:

$$P_m = (1 - R_U) - R_{delay} \tag{1}$$

where, R_U is the ratio of unsuccessful packet forwarding divided by the number of packets sent toward a node:

$$R_U = N_{dr} / N_s \tag{2}$$

where, N_{dr} is the number of dropped packets by a node and N_s is the number of packets sent towards the same node:

$$R_{delay} = N_{delay} / N_s \tag{3}$$

where N_{delay} is the number of packet which are delayed by a node and N_s is the number of packets sent towards the same node. By substituting the value of Equation (2) and Equation (3), the probability of a node being malicious is calculated. The calculated probability may be slightly different from the original behavior of the node, but the behavior of a node will fluctuate around this probability value.

After the probability has been calculated the trust evaluation process starts. The trust evaluation requires the values of forwarding sincerity, energy depletion and acknowledgement sincerity. Suppose there are two nodes *i* and *j* for which we want to calculate the values of these parameters. The forwarding sincerity (*F(i, j)*) is calculated as follows:

$$F(i,j) = \frac{SF_{(i,j)}}{SF_{(i,j)} + UF_{(i,j)}}(1 - P_m) \tag{4}$$

where, *SF(i,j)* is the number of successful packet forwarding from *i* to *j* and *UF(i,j)* is the number of unsuccessful packet forwarding from *i* to *j*. The acknowledgement sincerity has been calculated as follows. Here, *SACK(i,j)* and *UACK(i,j)* are the number of successful and unsuccessful acknowledgement forwarding respectively:

$$ACK(i,j) = \frac{SACK(i,j)}{SACK(i,j) + UACK(i,j)}(1 - P_m) \tag{5}$$

Energy is the important factor in WSN and should be conserved to improve the lifetime of the network. Hence, in the trust value calculation for TEAROR, the energy depletion (E_{impact}) has been introduced which is being calculated as follows:

$$E_{impact}(i,j) = \frac{E_{Fwd}(j) + E_{Rcv}(j) + E_{ack}(i,j)}{E_{total}(j)}(1 - P_m) \tag{6}$$

where, $E_{Fwd}(j)$ is the energy required by node *j* to forward a packet further to its neighbors. Similarly, $E_{Rcv}(j)$ is the energy required by node *j* to receive the packets from node *i* and $E_{ack}(i,j)$ is the energy consumed in sending acknowledgement from *j* to *i*. $E_{total}(j)$ is the total energy of the node *j*. this factor will tell about the impact of one transmission from node *i* to node *j*, on node *j*. If the impact is high, the trust value will be low. This will help in distributing the energy consumption among all the nodes.

After, all of sincerity factors are calculated, trust value will be computed. The trust value involves the aging factor. Each node has the formerly computed trust value for each neighbor. Hence, it must be included with recently calculated trust value (Salehi et.al., 2014). This is to be done because the sensor nodes, during their lifetime, may change their behavior. The newly computed trust value will help in monitoring the behavior of the nodes in the network. Following Equation (7) will calculate the new trust value (*RT(i,j)*) for node *j* with respect to node *i*:

$$RT(i,j) = \frac{\alpha * F(i,j) + \beta * E(i,j) + \gamma * ACK(i,j)}{\alpha + \beta + \gamma} \tag{7}$$

where α, β and γ are the importance factors. Means whichever sincerity factor out of three is most importance will be multiplied with highest value. By including previous behavior of the node *j* Equation (8) gives the final trust value (*FT(i,j)*) for node *j* with respect to node *i*:

$$FT(i,j) = \sigma * NewRT(i,j) + \lambda * (1-\sigma) * OldRT(i,j) \tag{8}$$

where, $0<\sigma<1$ represents the aging factor and $0<\lambda<1$ represents the weight of the *NewRT(i,j)*. These factors may be set to a value according to the simulation scenario and application of the network. In this way the final trust value has been calculated and used in relay selection algorithm which is being discussed in next subsection.

3.1.2. Relay Selection Algorithm

In opportunistic routing the relay selection out of some potential forwarders is very important task. Although, each potential forwarder have the opportunity to send data packet towards base station, but relay selection algorithm will decide the node which will forward the packet first. If this algorithm is not used than each node in the forwarder list will forward the data packets and base station will receive multiple duplicate packets. To monitor the packet transmission process, data packet forwarding progress (*FP*) is calculated using distance between source and destination ($D_{s,d}$) and distance between the destination and relay nodes($D_{ni,d}$) (Equation (9) and Equation (10)). Here, *k* is the total number of nodes in the network:

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \text{ , where } 0 \le i,j \le k \text{ , and } i \ne j \tag{9}$$

$$FP_{n_i}^{s,d} = D_{s,d} - D_{n_i,d} \text{, where s=source, d=destination, } 0 \le n_i \le k \tag{10}$$

The proposed relay selection algorithm below, starts at a random source node (*S*), which have data to be sent toward the base station (*D*). The list of 1-hop neighbor nodes for S has been formed. After forming this list, node trust factor (*FT*) has been calculated for each node in neighbor list. The value of *FT* will decide whether the node can be part of forwarder list (*FL*) or not. Sorting of the nodes in neighbor list is done by using the trust factor (*FT*). The nodes which are having *FT* value greater or equal to the minimum acceptable trust value (t_{min}) will be added to *FL*. But the capacity of *FL* will

be according to WSN application requirements. *FL* will be the list of potential forwarders, which can be trusted by the source node *S*. The data packets will be constructed including forwarder list and minimum trust value. Similar procedure will be followed by the receiver nodes. The node which is on the top of the forwarder list will forward the data packet first. The relay selection algorithm is the essential part of opportunistic routing process. This will decide the complexity of opportunistic routing process.

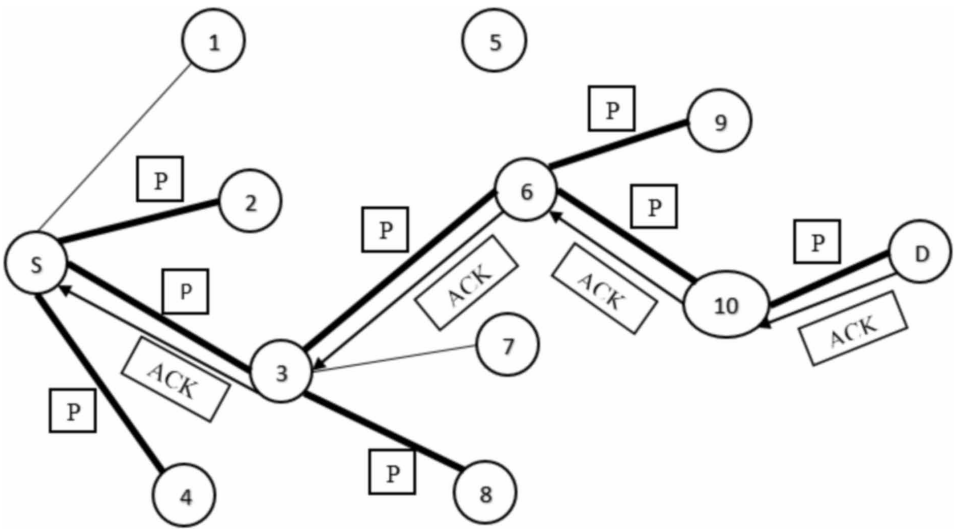
Consider the example network in Figure 1, which considers node *S* as source node and *D* as the destination node (base station). *S* will form its neighbor list as {1, 2, 3, 4} and calculate the trust value for each node in this list. Suppose the trust values for each node 1, 2, 3 and 4 are 0.2, 0.4, 0.6 and 0.4 respectively. The neighbor list will then be sorted according to trust values in descending order. After sorting the neighbor list will be {3, 2, 4, 1}. Now consider the number of forwarder nodes allowed in forwarder list are 3. Then forwarder list *FL* will contain {3, 2, 4}. After the forwarder list is formed the data packet is transmitted by including this forwarder list, minimum allowed trust value and destination address. The node which is on the top of forwarder list, 3 in this case, will forward the data packet first by following the same procedure. This process will be continued until the destination *D* is not found.

In relay selection algorithm (Algorithm 1), every node in the forwarder list will get the opportunity to send packet toward destination. Some of the nodes which are malicious or selfish nodes will not be included in forwarder list, because of low trust value. Hence, the TAEROR protocol will avoid such nodes to be included in the routing process. The packet *P* will travel only through the trusted nodes. Like in Figure 1, node 1 in the neighbor list of S will not be included in the forwarder list because of having low trust value. Similar is for node 7. Also, as only the top node on forwarder list is allowed to send packet further first, there will be no or very less duplicate packets received at destination (see Figure 2).

4. EXPERIMENTAL RESULTS AND ANALYSIS

TAEROR has been tested through extensive simulations on NS2 by creating simulation scenario. The simulation parameters' settings are shown in Table 1. The performance of TAEROR has been compared to existing trust aware routing protocols for WSN i.e. Trust and location aware routing

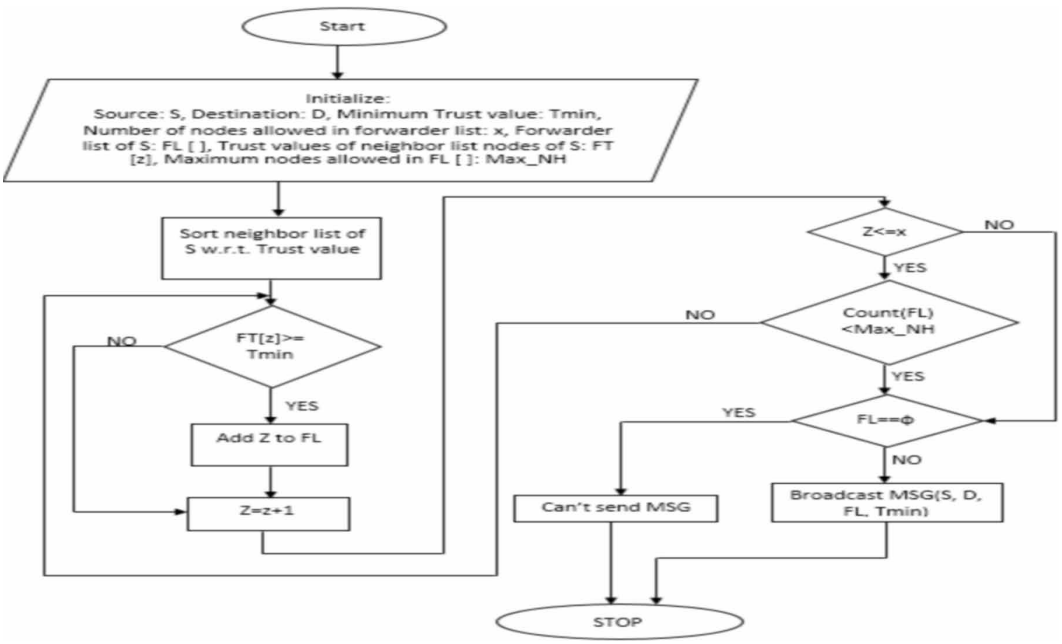
Figure 1. Example scenario of relay selection in TEAROR



Algorithm 1. Relay selection (S = Source, D = Destination)

```
When node S want to send a packet
Let t_min be the minimum acceptable trust factor of a node
x be the number of 1-hop neighbors of S
Let FT[Z] be the node trust factor of node Z
Let Max_NH be the maximum number of neighbors which are allowed
in forwarder list (FL)
FL= empty
Sort all 1-hop neighbors of S in descending order according to
FT[Z]
For (Z=1; FL < Max_NH and Z <= x; Z=Z+1)
Do
       If (FT[Z] >= t_min) then
                  Add Z's ID in FL
       EndIf
EndFor
If (FL!=empty)
       Broadcast MSG (S, D, FL, t_min)
EndIf
```

Figure 2. Flowchart for proposed relay selection algorithm



(TLAR) (Vamsi and Kant, 2016), Trust and energy aware secure routing protocol (TESRP) (Ahmed et al., 2016) and Trust aware opportunistic routing Framework (TAOR) (Salehi and Boukerche, 2014). All of these protocols are recently proposed protocols for wireless and sensor networks. The simulation settings shown in Table 1 has been applied to all compared protocols. The existing

Table 1. Simulation settings

Parameter	Value
Simulator	NS-2.35
Area of Deployment	500 x 500 m^2
Transmission Range	60 m
No. of Nodes (N)	25, 50, 100
No. of Malicious nodes	10, 20, 30, 40 and 50
Traffic Type	CBR (Constant Bit Rate)
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	100J
Initial Trust Value	1
Default σ and ʎ	0.90 and 0.4
Energy dissipation to run the radio ($E_{electronic}$)	50 nJ/bit

protocols i.e. TLAR (Vamsi and Kant, 2016), TESRP (Ahmed et al., 2016) and TAOR (Salehi and Boukerche, 2014) are re-implemented in NS2.

The simulation performance of all protocols has been tested in presence of black-hole and grey-hole attacks. Malicious nodes and selfish nodes has been created in the simulation environment based on the assumptions of proposed TAEROR protocol. The sensor nodes are assumed to be randomly deployed in area to be monitored. The malicious or selfish nodes do no generate any data packets, and also produce false network information. Black hole attack is created when the malicious node drops all of the packets coming to them. And grey hole attack is generated when selective packets has been dropped.

After completing extensive simulations for all protocols, the performance has been recorded and presented in form of graphs. The results are purely simulation based and all three protocols were tested on the same platform with same parameters. The security performance has been tested by using number of malicious nodes encountering during the routing process (Figure 3). As the routing is based on trust value, the nodes which are having very low trust values must be excluded during routing process. Proposed protocol TAEROR do the same thing. On the basis of forwarding sincerity values the nodes which are not forwarding the data packets i.e. implementing black-hole attack or grey-hole attack, will be excluded from routing path. Hence, there will be lesser number of malicious nodes encountered during routing process. Similar procedure has been followed by TLAR (Vamsi and Kant, 2016), hence it will present similar results. TESRP (Ahmed et al., 2016) and TAOR also calculated the forwarding sincerity values of nodes to avoid including malicious nodes into routing process. But the selfish nodes cannot be detected in these protocols.

The packet delivery ratio (Figure 4) also increase when any protocol is able to avoid black-hole and grey-hole attacks. This is because the number of retransmissions will be lesser. The proposed protocol TAEROR avoid the malicious nodes to be selected as the next-hop forwarder and hence secure the network from black-hole and grey-hole attacks. Similarly, TLAR (Vamsi and Kant, 2016) also do the same thing, but, it also used the feedbacks from other nodes and obviously, the nodes which are malicious will give positive feedbacks for other malicious nodes and negative feedbacks for good/healthy nodes. TAOR (Salehi and Boukerche, 2014) gives better results, but fails in providing energy efficiency. Similar is the case with TESRP (Ahmed et al., 2016).

Figure 3. Performance on the basis of average risk level

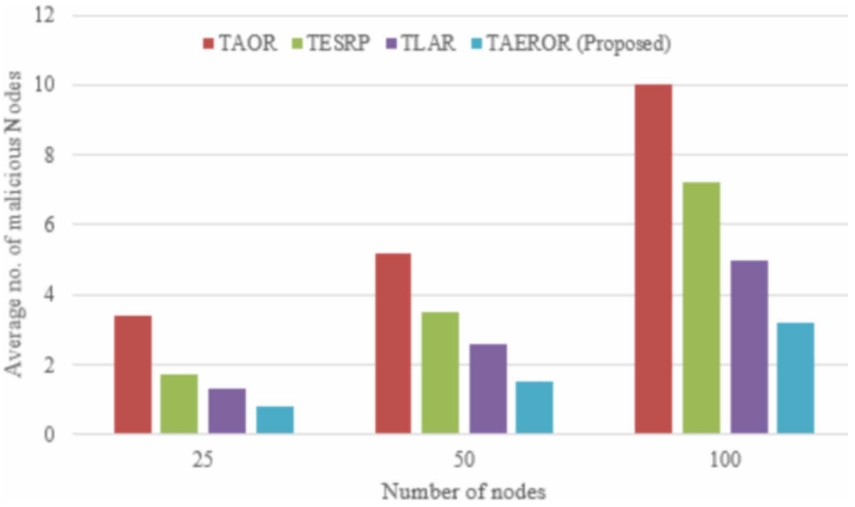
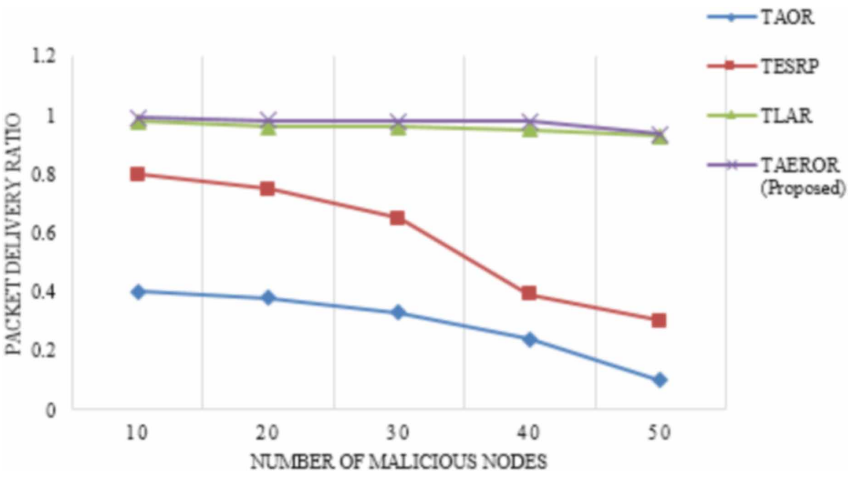


Figure 4. Performance on the basis of packet delivery ratio



The end-to-end delay (Figure 5) is also a major performance factor and all the protocols has been tested for the same. It is calculated as the total time consumed to deliver a data packet at destination node, when same packet is initiated from source node. End-to-end delay will be calculated only for successful packet deliveries. End-to-end delay will be high if greater number of malicious nodes encountered during routing process and also if overhead of selection of next-hop forwarder is high. TAEROR and TAOR (Salehi and Boukerche, 2014) calculate only direct trust values and avoid malicious nodes to be selected as next-hop forwarder, that's why the end-to-end delay is low. But, in case of TLAR (Vamsi and Kant, 2016) and TESRP (Ahmed et al., 2016) there will be overheads of calculating trust values and hence introduces more delays.

Energy consumption (Figure 6) is an important performance measurement factor in WSN. Energy consumption will decide the lifetime of the network. The major energy consuming processes in routing are transmitting and receiving packets and acknowledgements in the network. TAEROR, the proposed protocol considers all of these energy consumptions in the trust factor calculation

Figure 5. Performance on the basis of end-to-end delay

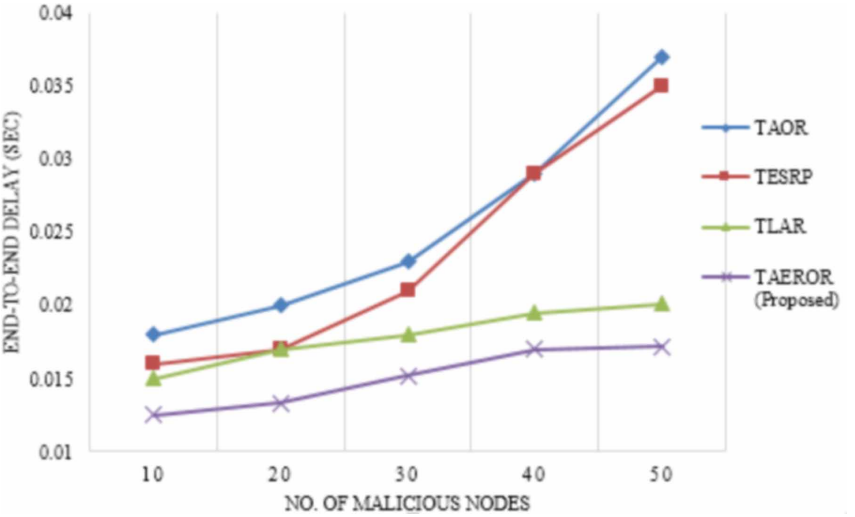
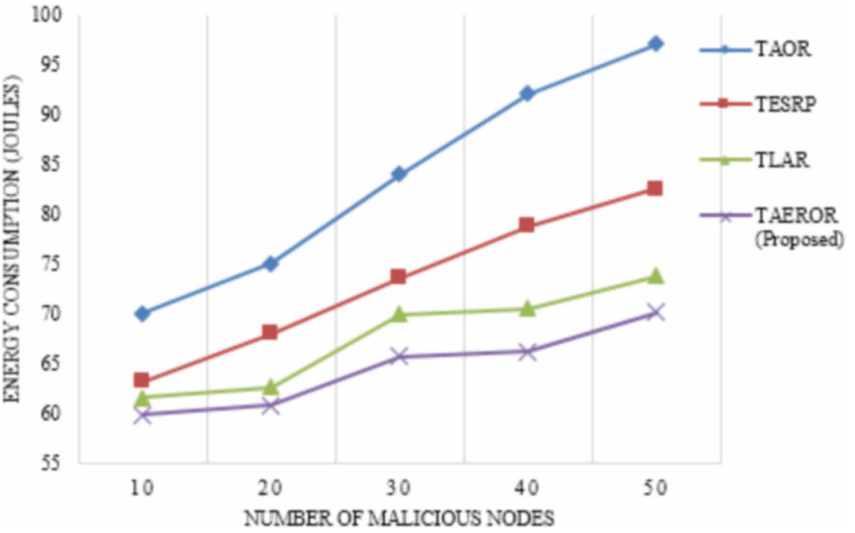


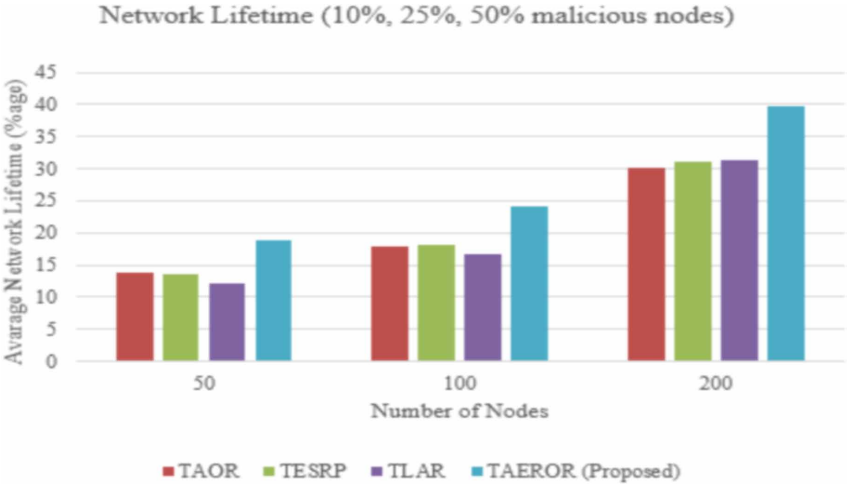
Figure 6. Performance on the basis of total energy consumption



and hence consume very less energy as compared to other algorithms. The overhead of trust factor calculation is also less because of simple calculations. The network lifetime also increases because of less energy consumption in the network.

There are different measures through which the network lifetime can be calculated. One way is to wait for the whole sensor nodes to decay their energy. Another way is when one node is dead the network is considered to be dead. In this paper for all compared protocols the average network lifetime has been calculated by using the percentage of number of nodes still alive even after the network is considered to be dead. The network is considered to be dead when the nodes stops communicating data packets towards the base station. The network lifetime has been checked for different number of nodes and in the presence of different number of

Figure 7. Network lifetime



malicious nodes. The proposed protocol presents better network lifetime than others because of less energy consumption. Also, the energy consumption is distributed among all nodes through trust value (see Figure 7).

5. CONCLUSION AND FUTURE SCOPE

Opportunistic routing is gaining popularity in wireless network types, especially for wireless sensor networks. Most of the opportunistic routing protocol proposed for WSN has not considered security as major issue. Also in WSN, the traditional security methods like cryptosystems, cannot be used because of lack of resources. Hence, in this paper a trust aware opportunistic routing protocol TAEROR is proposed, which is avoid malicious nodes to be involved in routing process. A trust calculation factor is proposed which considers forwarding sincerity, energy consumption and acknowledgement sincerity as major factors. A relay selection algorithm is also the part of protocol, which used the trust values to decide which node is qualified to take part in routing process. The trust value introduction in relay selection algorithm, secure the network from black-hole and grey-hole attacks. Simulation results shows the good performance of proposed protocol as compared to other recently proposed protocols i.e. TLAR, TAOR and TESRP. In future directions, we can consider more parameters in trust value calculation, but the more the parameters more will be computational overhead. Hence, only those parameters should be considered which seem to be important in the network like energy, packet delivery, etc.

REFERENCES

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. doi:10.1007/s11036-016-0683-y

Biswas, S., & Morris, R. (2005). ExOR: Opportunistic multi-hop routing for wireless networks. *Computer Communication Review*, *35*(4), 133–144. doi:10.1145/1090191.1080108

Channa, M. I., & Ahmed, K. M. (2011). A Reliable Routing Scheme for Post-Disaster Ad Hoc Communication Networks. *Journal of Communication*, *6*(7), 549–557.

Choudhury, S., Roy, S. D., & Singh, S. A. (2008). Trust management in ad hoc network for secure DSR routing. In *Novel algorithms and techniques in telecommunications, automation and industrial electronics* (pp. 495-500).

Cordasco, J., & Wetzel, S. (2008). Cryptographic versus trust-based methods for MANET routing security. *Electronic Notes in Theoretical Computer Science*, *197*(2), 131–140. doi:10.1016/j.entcs.2007.12.022

Darehshoorzadeh, A., & Cerda-Alabern, L. (2012). Distance progress based opportunistic routing for wireless mesh networks. *Paper presented at the 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*. doi:10.1109/IWCMC.2012.6314199

Deng, H., Yang, Y., Jin, G., Xu, R., & Shi, W. (2010). Building a trust-aware dynamic routing solution for wireless sensor networks. *Paper presented at the 2010 GLOBECOM Workshops (GC Wkshps)*. IEEE. doi:10.1109/GLOCOMW.2010.5700197

Dubois-Ferrière, H., Grossglauser, M., & Vetterli, M. (2011). Valuable detours: Least-cost anypath routing. *IEEE/ACM Transactions on Networking*, *19*(2), 333–346. doi:10.1109/TNET.2010.2070844

Füßler, H., Widmer, J., Käsemann, M., Mauve, M., & Hartenstein, H. (2003). Contention-based forwarding for mobile ad hoc networks. *Ad Hoc Networks*, *1*(4), 351–369. doi:10.1016/S1570-8705(03)00038-6

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, *4*(3), 15. doi:10.1145/1362542.1362546

Gheorghe, L., Rughinis, R., & Tataroiu, R. (2013). Adaptive trust management protocol based on intrusion detection for wireless sensor networks. *Paper presented at the Networking in Education and Research, 2013 RoEduNet International Conference* (12th ed.). doi:10.1109/RoEduNet.2013.6714201

Gong, P., Chen, T. M., & Xu, Q. (2015). ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks. *Journal of Sensors*.

Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys and Tutorials*, *14*(2), 279–298. doi:10.1109/SURV.2011.042711.00083

Haque, M., Pathan, A.-S. K., Hong, C. S., & Huh, E.-N. (2008). An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks. *Transactions on Internet and Information Systems (Seoul)*, *2*(5), 265–279. doi:10.3837/tiis.2008.05.004

He, Q., Wu, D., & Khosla, P. (2004). SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. *Paper presented at the Wireless communications and networking conference WCNC '04*. IEEE.

Hsu, C.-J., Liu, H.-I., & Seah, W. K. (2011). Opportunistic routing–A review and the challenges ahead. *Computer Networks*, *55*(15), 3592–3603. doi:10.1016/j.comnet.2011.06.021

Hu, Y.-C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, *1*(1), 175–192. doi:10.1016/S1570-8705(03)00019-2

Hu, Y.-C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, *11*(1-2), 21–38. doi:10.1007/s11276-004-4744-y

Kumar, N., & Singh, Y. (2016). An energy efficient and trust management based opportunistic routing metric for wireless sensor networks. *Paper presented at the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. doi:10.1109/PDGC.2016.7913196

Kumar, N., & Singh, Y. (2016). An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks. *Indian Journal of Science and Technology*, *9*(32). doi:10.17485/ijst/2016/v9i32/100197

Kumar, N., & Singh, Y. (2017). Routing protocols in wireless sensor networks. In Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures (pp. 86-128).

Liu, K., Abu-Ghazaleh, N., & Kang, K.-D. (2007). Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, *67*(2), 215–228. doi:10.1016/j.jpdc.2006.08.001

Liu, Z., Wei, C., Qin, C., Li, H., Niu, X., & Wang, L. (2013). POR: A Packet-Based Opportunistic Routing Protocol for Wireless Sensor Networks. *Paper presented at the 2013 International Conference on Computer Sciences and Applications (CSA)*. doi:10.1109/CSA.2013.43

Maarouf, I., Baroudi, U., & Naseer, A. R. (2009). Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks. *IET Communications*, *3*(5), 846–858. doi:10.1049/iet-com.2008.0324

Mantas, N., Louta, M., Karapistoli, E., Karetsos, G. T., Kraounakis, S., & Obaidat, M. S. (2017). *Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey*. IET Networks.

Michiardi, P., & Molva, R. (2002). *Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks Advanced communications and multimedia security* (pp. 107–121). Springer.

Mohaisen, A., Choi, J. W., & Hong, D. (2009). On the insecurity of asymmetric key-based architecture in wireless sensor networks. *Transactions on Internet and Information Systems (Seoul)*, *3*(4), 376–384. doi:10.3837/tiis.2009.04.003

Rozner, E., Seshadri, J., Mehta, Y., & Qiu, L. (2009). SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks. *IEEE Transactions on Mobile Computing*, *8*(12), 1622–1635. doi:10.1109/TMC.2009.82

Salehi, M., & Boukerche, A. (2014). Trust-aware opportunistic routing protocol for wireless networks. In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks* (pp. 79-86). doi:10.1145/2642687.2642692

Salehi, M., Boukerche, A., Darehshoorzadeh, A., & Mammeri, A. (2016). Towards a novel trust-based opportunistic routing protocol for wireless networks. *Wireless Networks*, *22*(3), 927–943. doi:10.1007/s11276-015-1010-4

Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *20*(11), 1698–1712. doi:10.1109/TPDS.2008.258

Srinivasan, A., Teitelbaum, J., & Wu, J. (2006). DRBTS: distributed reputation-based beacon trust system. *Paper presented at the 2nd IEEE international symposium on Dependable, autonomic and secure computing*. doi:10.1109/DASC.2006.28

Tanachaiwiwat, S., Dave, P., Bhindwale, R., & Helmy, A. (2004). Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. *Paper presented at the 2004 IEEE International Conference on Performance, Computing, and Communications*. doi:10.1109/PCCC.2004.1395061

Vamsi, P. R., & Kant, K. (2016). Trust and location-aware routing protocol for wireless sensor networks. *Journal of the Institution of Electronics and Telecommunication Engineers*, *62*(5), 634–644. doi:10.1080/03772063.2016.1147389

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, *52*(12), 2292–2330. doi:10.1016/j.comnet.2008.04.002

Zahariadis, T., Trakadas, P., Leligou, H. C., Maniatis, S., & Karkazis, P. (2013). A novel trust-aware geographical routing scheme for wireless sensor networks. *Wireless Personal Communications*, *69*(2), 805–826. doi:10.1007/s11277-012-0613-7

Zhang, K., Wang, C., & Wang, C. (2008). A secure routing protocol for cluster-based wireless sensor networks using group key management. *Paper presented at the 4th International Conference on Wireless Communications, Networking and Mobile Computing WiCOM'08*. doi:10.1109/WiCom.2008.889

Zhong, Z., Wang, J., Nelakuditi, S., & Lu, G.-H. (2006). On selection of candidates for opportunistic anypath forwarding. *Mobile Computing and Communications Review*, *10*(4), 1–2. doi:10.1145/1215976.1215978

Zhou, Y., Tan, X., He, X., Qin, G., & Xi, H. (2010). Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature. *Information Assurance and Security Letters*, *1*, 18–23.

Nagesh Kumar is currently pursuing a PhD from Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India. The author received an MTech in Computer Science from Himachal Pradesh University, Shimla (HP), India. Nagesh's area of interests are Wireless Sensor Network, Internet and QoS routing.

Yashwant Singh is currently working as Associate Professor in Department of Computer Science & IT at Central University of Jammu, Jammu and Kashmir. He has 12 years of experience in academics at reputed Colleges and Universities in India. He has completed his PhD in Computer Science from Himachal Pradesh University, Shimla, H.P., India. He received his Master of Engineering from Punjab Engineering College, Chandigarh, India. He has obtained his Bachelor of Engineering from SLIET, Longowal, Punjab, India. Dr. Singh is a Member of IEEE, Member CSI, Member ACM and Life Member of ISTE. He was general chair IEEE PDGC-2014 and associated as TPC member, session chair & reviewer of various Conferences & Journals in India and abroad.

Pradeep Kumar Singh is currently working as an Assistant Professor (Senior Grade) in Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT), Waknaghat, H.P. He has 10 years of vast experience in academics at reputed colleges and universities of India. He has completed his PhD in Computer Science & Engineering from Gautam Buddha University (State Government University), Greater Noida, UP, India. He received his MTech (CSE) with Distinction from Guru Gobind Singh Indraprastha University, New Delhi, India. He has obtained his BTech (CSE) from Uttar Pradesh Technical University (UPTU), Lucknow, India. Dr. Singh has life membership of Computer Society of India (CSI) and promoted to Senior Member Grade from CSI. He is member of ACM, IACSIT-Singapore and IAENG-Hong Kong. He has worked as publicity chair of five IEEE International Conferences and associated as TPC member & reviewer of various Conferences & Journals too.