Asian Journal of Information Technology 15 (4): 817-824, 2016
ISSN: 1682-3915

Modelling of Confidential Data Forwarding Based on Trust Management in Wireless Sensor Networks

[1]P.N. Renjith and [2]E. Baburaj
[1]Department of Computer Science and Engineering,
Lord Jegannath College of Engineering and Technology, Marungoor,
[2]Department of Computer Science and Engineering,
Narayanaguru College of Engineering, Manjalumoodu, Kanyakumari District, Tamil Nadu, India

Abstract: Enormous innovations in wireless communication have made outstanding enhancements in the arena of Wireless Sensor Networks (WSN). Today, WSN has been transformed into an inevitable technology and controls virtually all the applications like ecological monitoring, security and application that save our lives and possessions. Unlike the conventional wired Network, WSN has its own unique characteristics which make WSN distinctive and more feasible. The WSN is an infrastructure-less network and it utilizes a large range of sensor nodes which can be deployed in a specific geographical area of interest to sense and gather information. These information are forwarded to the base station with the help of a routing protocol. The physical nature of WSN with its limited battery, processing and communication capacity makes it unique and susceptible to external attacks like snooping, eaves dropping and many other attacks. In this research study, a new Trust Evaluation (TEV) protocol for sensor network security has been implemented based on nodes reputation within the network. The TEV protocol can effectively evaluate the nodes' misbehavior and commendably extricate the normal and malevolent behavior. Simulation results prove that the performance of sensor nodes has improved with better security and limited energy utilization.

Key words: Security, trust evaluation, wireless sensor, index terms, nodes, battery

INTRODUCTION

Incredible advancement in MEMS have favored a fabulous growth in Wireless Sensor Networks (WSN). WSN is an Ad-hoc network and it works in collaboration with hundreds to thousands of wireless sensor nodes. These sensor nodes are deployed in an explicit topographical range of attention so as to observe the physical or environmental conditions such as temperature, sound, vibration, pressure or pollution (Akyildiz *et al*., 2002; Tilak *et al*., 2002; Bharathidasan and Ponduru, 2002; Rentala *et al*., 2002; Weatherall and Jones, 2002). These sensed data are dispatched in the form of packets to their destination with the help of multi-hop communication. The WSN follows the principles of multi-hop communication and hence, each wireless sensor node has to participate deliberately for both in transmission of data or act as a relay in transmission of data. Figure 1 represents the working of wireless sensor networks. All the communication between the source and destination pass through several intermediate nodes.

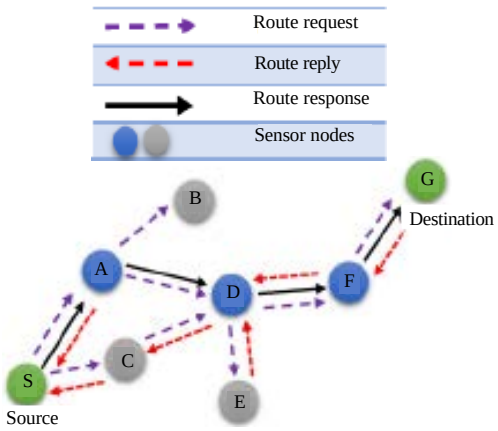

Fig. 1: Wireless sensor network

Each intermediate nodes act as a router (Akyildiz *et al*., 2002; Tilak *et al*., 2002; Bharathidasan and Ponduru, 2002) to transmit and forward packets generated by the node and its neighbors. Each sensor node forwards the sensed information in a form of packets from

Corresponding Author: P.N. Renjith, Department of Computer Science and Engineering,
Lord Jegannath College of Engineering and Technology, Marungoor, Kanyakumari District, Tamil Nadu, India

one node to another (multi-hop routing), it passes several intermediate nodes to reach its destination. On account of lack of co-operation among the sensor nodes caused by selfishness or malevolence the network performance is affected. This routing operation of a sensor node can be counterfeit by the malevolent attack. Intruders target on this routing operation of the sensor node which can lead to entire network collapse.

Trust evaluation is considered as an invincible requirement for proper routing in a complex network with heterogeneous nodes (Chen, 2009). It is also an important aspect in route decision making (Liu *et al*., 2009). Khalid *et al*. (2013) based on their comparative studies, trust management should be considers as pre-routing issue in wireless sensor networks. By clarifying the trust relationship, it will be easier to take proper routing issues. Degradation in network performance is noted due to selfish or malice behavior of the sensor nodes. Once, the sensor node is compromised to an external attacker the intruder can inject false data and forward them into the network. It is also noted that the sensor nodes are reprogrammed to carry out various tasks that may ultimately rescind the entire network. In WSN, the trust between the sensor nodes plays a major role in incessant communication (Bhattacharyya *et al*., 2010; Lewis, 2004). Cryptographic technique may be the best solution for conventional networks with maximum battery resource and extensive computational power like mobile network or wired network. In wireless sensor networks, sensor nodes are deployed with limited battery power, computational power, processing bandwidth and storage (Khalid *et al*., 2013). Therefore, sensor nodes cannot support the computational complex cryptographic protocol. On the other hand, trust management method has universally been accepted as a technique to compute the nodes Trust worthiness by direct and indirect evaluation. Trust evaluation is done by the present and past experiences of a sensor node and making a decision in uncertainty whether the specific node is suitable for data forwarding or communicating. A sensor node will participate in the data communication only if holds good reputation by its neighboring nodes (Khalid *et al*., 2013; Chen, 2009; Liu *et al*., 2009; Arenas *et al*., 2010). Hence, trust management protocol can be considered as a vital characteristics determines overall goodness of the network which includes, network lifetime, through put and confidential data forwarding.

Literature review: In this study, an exploration on the existing studies on trust management in wireless network was done. Extensive research works have been carried out on trust evaluation in wireless networks. Researchers have adopted different techniques while calculating the trust between nodes deployed. Among them majority of the research relay on direct and indirect trust evaluation. Buchegger and Boudec (2002) have performed an analysis on cooperation of nodes fairness in dynamic adhoc networks, based on direct and indirect trust evaluation. The CONFIDENT protocol adds weightage to the indirect trust value. Analysis prove that CONFIDENT protocol has avoided false praising attacks. Result and discussion prove that the improved DSR routing protocol works seamlessly well in malicious node networks. However, CONFIDENT protocol may entitle bad mouth attack as the indirect trust value was given with higher priority.

Chen (2009) has proposed Task-based Trust for Sensor Networks (TTSN). The TTSN protocol is computed using Bayesian theorem and beta distribution. The TTSN takes a different approach based on the tasks performed by the sensor nodes. Initially, the trust value of sensor nodes deployed are marked as neutral. Direct trust value is considered for evaluating trust between the sensor nodes. The TTSN secures the network from ballot attack and bad mouth attack. Studies prove that TTSN takes a higher learning time to build a trusted network as it depends on direct trust evaluation. Zahariadis *et al*. (2010a) have presented a secure framework, Ambient Trust Sensor Routing (ATSR) for wireless sensor networks with the sensor nodes deployed with neutral trust value, ATSR calculates the direct and indirect trust value based on the periodic request sent by the nodes. More weightage is assigned to distance metrics for trust evaluation. Studies prove that the packet drop rate is decreased; however, high communication overhead is generated due to the periodic trust request send between the nodes.

Michiardi and Molva (2002) have designed collaborative reputation mechanism to calculate the trust value in mobile network. The CORE has extended DSR routing protocol for trust evaluation. Each nodes is assigned with neutral trust values and computed trust values based on the weighted mean of direct and indirect node observations. The communication overhead of the network is increased due to the frequent contribution of the nodes. Liu *et al*. (2009) have designed Distributed Event-triggered Trust Management model (DETM) using cryptographic method where each sensor node is deployed with a neutral trust value. Data forwarding is done by encrypting the data using a private key. Trust values are updated using event-triggered information of the sensor nodes. Trust value is evaluated with Gaussian distribution method using direct and indirect node observations with higher weightage is assigned to energy metrics. The through put of the wireless sensor network may get degraded due to the computational complexity of the cryptographic techniques.

Pandarinath *et al*. (2010) have presented a new light weight secure trust-based localization method to evaluate trust and detect the malicious nodes based on the location information of the sensor nodes in wireless sensor networks. In this practice, sensor nodes are initialized with a neutral trust value. Distance estimation technique is used to compute the trust where more weightage is given to the distance metrics considering the past experience of the nodes. Wireless sensor network may experience a higher memory utilization due to the storage of packet transmission and location information as they are equipped with limited memory resource.

Although, there are many researches on trust and reputation management in wireless sensor network, the task is still on an evolutionary stage in case of WSN. The sensor nodes are supplied with limited battery, memory and computational power. Utilization of complex algorithms and techniques in WSN degrades the network's lifetime.

Scalability is an on going research issue and it is a major challenge, since WSN consist of spatially disseminated sensor nodes, ranging from hundreds to thousands. Trust value may get debased with an increasing number of sensor nodes. Therefore, it is necessary to find competent trust management mechanism with high effective through put rate for such networks.

MATERIALS AND METHODS

Problem identification: This research study intend to design a trust based Wireless Sensor Networks (WSN) in which data confidentiality can be effectively attain with trust evaluation mechanism. To ensure secure data sensing and forwarding, trust management technique has to be initialized immediately after sensor node deployment. The trust management protocol will enable the sensor nodes to perform secure communication with the trusted nodes. Trust Evaluation protocol (T_{EV}) is as an addition to reactive routing protocol in wireless sensor networks. Adhoc on-demand distance vector routing protocol is used as a base routing protocol. Perkins and Royer (1999) has proposed Adhoc on-demand distance vector routing protocol (Bhat *et al*., 2011), a reactive type routing protocol to perform routing using event based technique. AODV utilizes events, like route request (RREQ), Route Reply (RREP) Route Error (RERR). Route Request is sent by the source node to discover a route between the source and destination. Route reply is sent by the destination node to reply to the source node. Route error is an error message stating the route failure and initiates the source node to rediscover a new route between the source and destination. AODV is a flat routing protocol which does not require any central administration process to maintain routing (Perkins and Royer, 1999). Hence, AODV routing protocol is extended in this proposal integrating trust mechanism. Trust is a grade obtained by a sensor node by the present and past experiences which can perform the secure routing with minimum losses. Trust management procedure can be functional on WSN with heterogeneous sensor nodes with varying energy levels and altered gradations of malicious and selfish activities. Trust evaluation mechanism will assist to adopt the finest reliable route for data forwarding among the nodes. Trust evaluation is determined by trusted nodes, trust values, main Trust (mT_{EV}), ancillary Trust (aT_{EV}) and trust factors (Mahoney *et al*., 2005; Zahariadis *et al*., 2010b). Trust management proposed in this study is event based, i.e., trust evaluation is done by recording the sequences of events executed by the sensor nodes. The sensor nodes normally send, receive, failure transmitting, failure receiving packets. In trust evaluation, following sensory events, like Packet Transmission (PK_{Tx}), Packet Received (PK_{Rv}), Packet Transmission Error ($PK_{Tx}E$) and Packet Received Error ($PK_{Rv}E$) are used with different trust metrics like packet delivery factor, sensor node availability, battery lifetime, through put and packet delay. Trust evaluation is done in two ways. Main trust evaluation and ancillary trust evaluation. In Main trust evaluation, sensor node within its range are evaluated and trust value is calculated. Ancillary trust evaluation is recommended trust value of a sensor node by other sensor nodes which resides beyond its range of communication. Summation of mT_{EV} and aT_{EV} will provide TEV for the sensor node. Trust evaluation is time based hence, trust evaluation will be made in regular intervals of time. Once, the sensor nodes are deployed, each sensor node broadcasts there "hello message" to identify the neighboring nodes. In this study, the "hello message" is replaced with trust packet. These trust packets are utilized for trust calculation. Each trust packet transmitted by a N_i to N_j should be received back from $N_{j,j}$. Loss in the packet or delay will affect the trust worthiness of N_j. Let, $Pk_{tx i->j}$ be packet transmitted from Node I (N_i) to Node j (N_j) and $PK_{rv j->i}$ packet received by Node j (N_j) from Node i (N_i).

Sensor node Packet Delivery (PDα): Sensor node packet delivery enables to calculate the packet delivery between the two nodes i and j. Loss in the packet or delay would affect the trust worthiness of N_j. The packet delivery rate between the node i and node j $Pd_{\alpha i-j}$ is calculated with Eq. 1 using the packet transmitted and received rate at a given interval of time:

$$PD_{\alpha i\to j} \approx \frac{PK_{Rvj\to i} - PK_{RvEj\to i}}{PK_{Txi\to j} - PK_{TxEi\to j}} \quad (1)$$

Packet transmission Rate (Pr_β): Packet transmission rate helps to find the total number of packets transmitted $PK_{tx\ i->j}$ and received $PK_{rv\ j->i}$ by a sensor node at given interval of time T. The value is calculated by conducting experiments with standard setting at a given interval of time. Based on results of the several experiments γ value is chosen to be 0.53. The packet transmission rate can be calculated using Eq. 2:

$$PR_{\beta i\to j} \approx \frac{\sum_{i=0}^{n}\left(PK_{Txi\to j} + PK_{Rvj\to i}\right)}{15} \times \frac{1}{\gamma} \quad (2)$$

Sensor node Battery Lifetime (BL_{tot}): Let the SN is deployed at time tin with the battery level bin. At time T_{cu}, the battery level is B_{cu}. Battery utilized B_{util} is calculated by finding the difference between B_{in} and B_{cu}. Hence, approximate lifetime of sensor node BL_{tot} will be evaluated using Eq. 3:

$$BL_{tot} \approx \frac{B_{in}}{B_{in} - B_{cu}} \times \left(T_{cu} - T_{in}\right) \quad (3)$$

$$BP_{rem} = \frac{B_{cu}}{B_{in}} \quad (4)$$

End to end Delay (ED): Sensor nodes transmission gets delayed either due to the network complexity or any malicious activity. Delay can affect the entire network and it has to be controlled. End to end delay can be measured by finding the difference of transmission and receiving of packet between nodes. Let, $TPK_{Rvj\to i}$ time to receive packets from node j to i and $TPK_{Txi\to j}$ be time to receive packets from node i to j. Hence, End to end Delay ($ED_{i->j}$) can be calculated using Eq. 5 and 6:

$$ED_{i\to j} \approx \left(\left(\frac{TPK_{Txi\to j}}{TPK_{Rvj\to i}}\right)\right) \quad (5)$$

$$ED_{i\to j} = \begin{cases} \alpha_i \,\forall \text{ values ranging from } 0.7 \le \alpha \le 1 \\ 0 \text{ otherwise} \end{cases} \quad (6)$$

Trust evaluation $T_{EVi->j}$ is calculated using the Eq. 7 summation of sensor node Packet Delivery(PD_α), Packet transmission Rate (PR_β) End to end Delay ($ED_{i,j}$) and sensor node Battery Lifetime (BL_{tot}). Average $T_{EVi\to j}$ is evaluated by calculating total number of interactions (n) by node i with the node j. Main trust evaluation is calculated by the Eq. 8 and 9:

$$T_{EV\,i\to j} = \frac{1}{4}\sum\left(PD_{\alpha i\to j} + PR_{\beta i\to j} + ED_{i\to j} + BP_{rem}\right) \quad (7)$$

$$AVG^{T_{Evi\to j}} = \frac{1}{n}\left(T_{Ev\,i\to j}\right) \quad (8)$$

$$mT_{Ev}\left(_{i\to j}\right) = \frac{T_{Ev\,i\to j}}{AVG^{T_{Evi\to j}} + \sum\left|AVG^{MT_{EV}} - T_{Ev\,i\to j}\right|} \quad (9)$$

Ancillary Trust evaluation (αT_{EV}): Ancillary trust evaluation is the secondary trust evaluation based on recommendation. The αT_{EV} is the recommendation of a sensor node by the other neighboring sensor nodes:

$$\alpha T_{Ev} = \frac{1}{n}\sum\left(mT_{Ev(\alpha)} + mT_{Ev(b)} + \ldots + mT_{Ev(n)}\right) \quad (10)$$

Trust evaluation done by sensor node A on its neighbors. Table 1 describes main trust values mT_{EV}, Ancillary trust value αT_{EV} and trust evaluation value. Trust Evaluation (T_{EV}) trust evaluation is done as in a deep-rooted scheme by totaling the Main trust evaluation value along with the Ancillary trust evaluation value. Summation of the main trust evaluation and the ancillary trust evaluation will generate the final trust evaluation as shown in Eq. 11. However, the primacy factor (pf) determines the Ancillary trust evaluation value to be used based on the application. In most secure requisite applications, like border security, Ancillary trust value is given low priority. Trust evaluation will be done with consistent interval of time. Trust evaluation values will be stored in trust evaluation Table (Table 1) as shown in Eq. 12:

$$T_{Ev} = \frac{1}{2}\sum mT_{Ev} + pf\left(\alpha T_{Ev}\right) \quad (11)$$

$$T_{EvA\to B} = \left\{Nodel(B), mT_{Ev}, \alpha T_{Ev}, Aggregate\,T_{Ev}\right\} \quad (12)$$

Algorithm 1; Trust management:

Initialize Sensor Nodes (SN)
Evaluate mT_{EV} using Eq. 1-7
Generate mT_{EV} and αT_{EV} using Eq. 7 and 8
Compute $T_{EV\ A-B}$//Trust Evaluate (T_{EV}) the adjacent neighbors
Check $T_{EV} \ge$ Threshold (Thα)
if T_{EV}<THα
Add Nid to TG//adding a node to the trust group
Multicast the trust database of a node to the other nodes
Else Add Nid to UTG//adding a node to untrusted group
End if

Table 1: Model of trust evaluation table of sensor node a to its neighbors B-D

Sensor node ID	mT_{Ev}	αT_{Ev}	T_{Ev}
B	mT_1	aT_1	T_1
C	mT_2	aT_2	T_2
D	mT_3	aT_3	T_3

Clustering: Cluster based WSN network with multiple clusters is considered for T_{EV} algorithm. A cluster of sensor node is formed based on trust evaluation value and node distance. A cluster consists of Cluster Head (CH), secondary cluster head and sensor nodes. Cluster head is a sensor node and is elected based on its high residual power and resources than the other sensor nodes in the cluster. The cluster head is elected based on an election protocol such as in HEED (Pandarinath *et al*., 2010; Mariappan and Paramasivan, 2015). The node with the second maximum battery power is made the secondary cluster head.

Algorithm 2; Cluster head and secondary cluster head selection:

Check for neighbors based on TG and node distance
Initialize election message
Calculate BL_{tot} and BP_{rem} using Eq. 3 and 4
If Ni = Max BP_{rem} And Max T_{EV}
Make N_i as cluster head
If N_j has second BP_{rem} Max T_{EV}
Make N_j as secondary cluster head
Multicast CH and SCH information to neighboring nodes
End if

Table 2: Summary of notations

Notation	Explanation
T_{Ev}	Trust evaluation
BL_{tot}	Total battery life time
BP_{rem}	Remaining battery power
$TPK_{Tx\ i\text{-}j}$	Time stamp of packet transmitted from i->j
$TPK_{Rvj\text{-}i}$	Time stamp of packet received from j->i
mT_{Ev}	Main trust evaluation value
αT_{Ev}	Ancillary trust evaluation value
TH_{α}	Threshold value
Pf	Primacy factor

The sensor nodes sense the queried data by the user and forward them to the cluster head. The secondary cluster head aggregates the redundant data and forward them to the cluster head. The cluster head collects the data from all the secondary cluster heads and forward them to the base station or gateway node (Table 2).

RESULTS AND DISCUSSION

Performance evaluation and comparison: Trust evaluation algorithm has been executed on wireless sensor networks by conducting a wide-ranging simulation using Network Simulator (NS 2.35). Trust Evaluation algorithm is incorporated with all the sensor nodes and has deployed 100 nodes in a geographical area of 200×200 m^2. The CBR is used as the source traffic generator. The sensor nodes are deployed in to a scenario with malicious nodes at different densities ranging from 0-30% as shown in Fig. 2. The simulation result prove that the preprogrammed sensor nodes clearly isolate the malicious nodes based on the trust evaluation algorithm. In the initial phase of simulation, a slight delay is noted due to the learning process.

During the learning process, the sensor nodes perform trust evaluationon, its neighbor and the trust worth nodes are classified basedon the trust values. The performance of the routing protocol isimproved with increased network lifetime by avoiding retransmission. We implemented our Trust Evaluation algorithm with AODV (T_{EV} AODV) routing protocol. The AODV routing

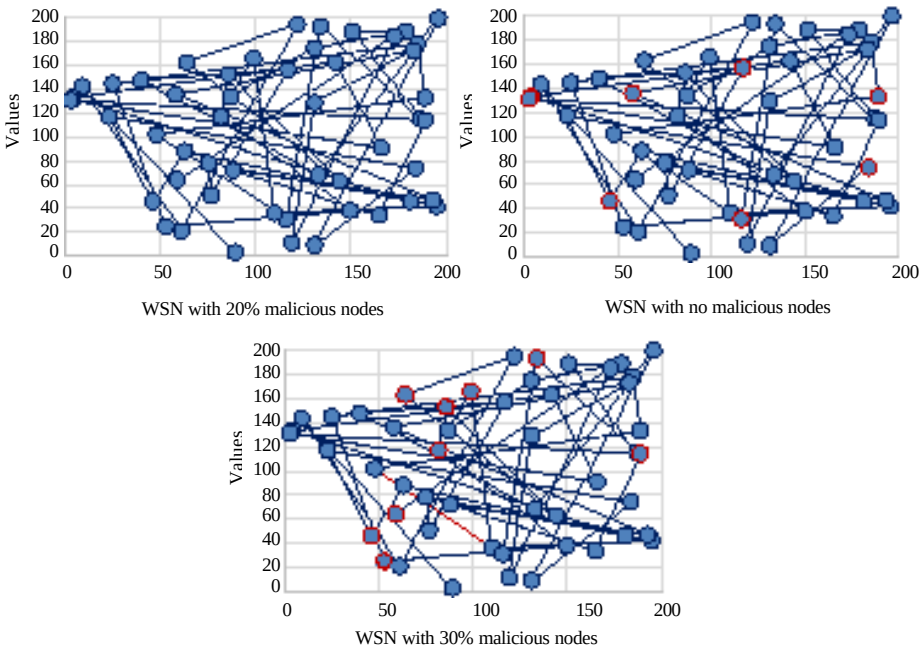

Fig. 2: Wireless sensor network with varying malicious node density

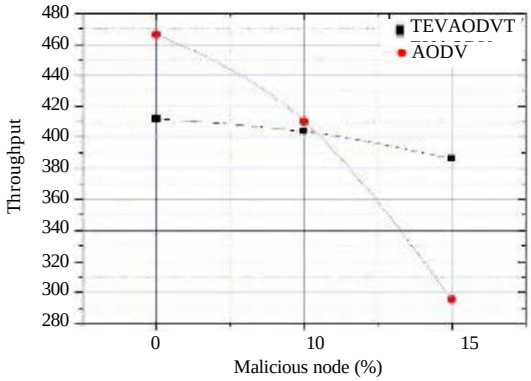

Fig. 3: Evaluation of through put between AODV and T_{EV} AODV

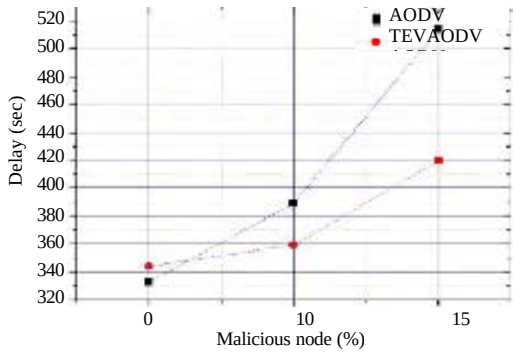

Fig. 4: Evaluation of Delay between AODV and T_{EV} AODV

protocol is reactive based routing protocol and comparative studies prove that AODV as the best routing protocol for Wireless Sensor networks. Trust Evaluation method added AODV routing protocol T_{EV} AODV exhibits better results when compared with the traditional AODV routing protocol. Simulation results prove that the performance of the sensor nodes has improved with better security and limited energy utilization.

Evaluation of throughput: Throughput is measured in terms of the successful deliveryof the data packet within the threshold time. Figure 3 explains through put of AODV and T_{EV} AODV with varying malicious node percentages. Initially with a lesser number of malicious nodes both routing protocols show a better result. However with an increase in the malicious node percentage, AODV shows very low through put. Based on the experimental study T_{EV} AODV has a higher through put of 8% than AODV routing protocol.

Evaluation of end to end delay: End to end delay performance metrics is used to measure the time taken by a pack to travel across a network from the source node to the destination node. The time includes the route discovery latency, queuing latency, retransmission delay at the MAC, propagation and transfer times. Figure 4 explains the performance of AODV and T_{EV} AODV routing protocol with different malicious node densities. The T_{EV} AODV takes more time but it is consistent in all the different node combination varying from 25-100. T_{EV} AODV initially utilize a period of time for computing trust evaluation. This will create a delay initially, however, the network life time and performance are improved by avoiding malicious activities within the nodes. Based on the experiment T_{EV} AODV has out performed AODV with 12% lesser delay.

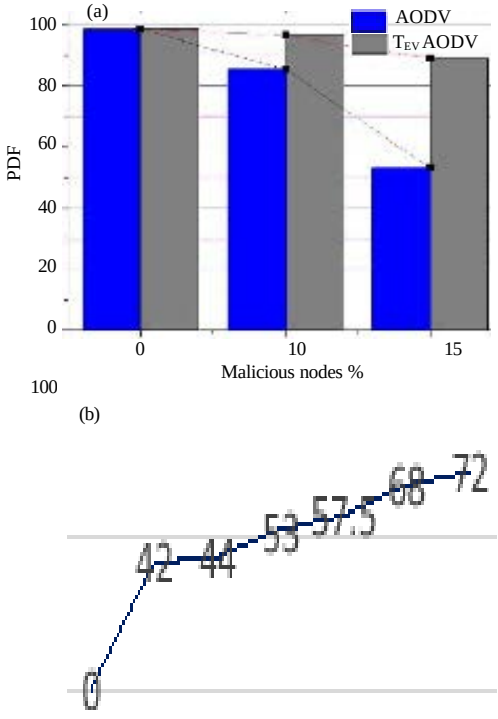

Fig. 5: Evaluation of Packet delivery ratio between AODV and T_{EV} AODV

Evaluation of packet delivery ratio: Packet delivery ratio helps to evaluate the total packets properly delivered. It is the ratio of the total amount of the data packets received at the destination to the total packet transmitted at the source. Figure 5 explains the graphical representation of the packet delivery ratio between AODV and T_{EV} AODV routing protocol with varying number of sensor nodes. The results are similar as previous experiments. The T_{EV}AODV routing protocol perform better than AODV routing protocol.

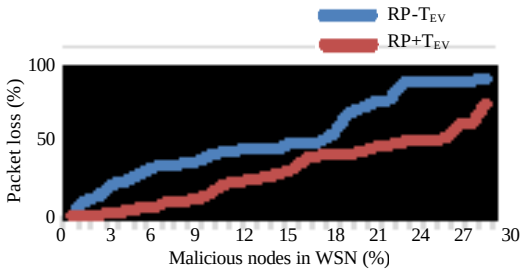

Fig. 6: Packet loss with increasing malicious nodes

Table 3: Failure prediction using graphical method

Routing Protocol (RP)	Aggregate packet loss	Graphically predicted packet loss	Percentage of error
RP-T_{EV}	81.18	82.45	-1.27
RP+T_{EV}	66.91	68.88	-1.97

Failure prediction using graphical method: A graphical method is used to predict the trust failure of Routing Protocol (RP) with trust evaluation and without trust evaluation. This is done by considering varying malicious node range of 0-30% and plotting the corresponding failures and packet loss of the WSN as in Fig. 6. The graph represents the performance of routing protocol with trust and without trust evaluation algorithm with increasing malicious node density. During the experiment, its noted routing protocol with trust evaluation performance getting degraded when the malicious node percentage increases beyond 27% due to unavailability of shortest and secure path to transmission.

Using IBM SPSS software the percentage of error with the actual failure routing protocol with trust evaluation and without trust evaluation are -1.97 and -1.27, respectively. The predicted failure load is as shown in Table 3. The WSN without trust evaluation that has recorded severe loss of packets in the earlier stage of attack whereas routing protocol with trust was able to withstand malicious attack.

CONCLUSION

Wireless sensor networks comprises heterogeneous sensor nodes which are often deployed in intimidating environment where possible failure due to the external attacks are considerably enlarged. It is proven that the sensor nodes get easily compromised to the external attacks with various studies. Injecting untruthful data in sensed information will result in big issues. Hence, implementing a trust mechanism similar to human society is best solution for majority of malicious attacks. In this research study, AODV routing protocol is extended with Trust Management algorithm (T_{EV}) and its performance is evaluated with traditional AODV. This method is adopted to accomplish confidential data forwarding with minimum retransmission.

Experimental results have proven that T_{EV} AODV has shown better results with varying sensor density. Moreover, the proposed trust management technique is light weighted, effective and robust and require less computational power. By reducing data losses and retransmissions, the battery energy can be conserved extensively. This will contribute to improved network life time. As future research, a real time test bed experiment is being intended with sensor nodes to evaluating the performance of trust algorithm.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. A survey on sensor networks. IEEE Commun. Mag., 40: 102-114.

Arenas, A.E., B. Aziz and G.C. Silaghi, 2010. Reputation management in collaborative computing systems. Secur. Commun. Networks, 3: 546-564.

Bharathidasan, A. and V.A.S. Ponduru, 2002. Sensor networks: An overview. Technical Report, Department of Computer Science, University of California, Davis, CA., USA. http://saluc.engr.uconn.edu/refs/sensornetwork/bharathidasan_sensor.pdf.

Bhat, S., D. Shwetha and J.T. Devaraju, 2011. A performance study of proactive, reactive and hybrid routing protocols using qualnet simulator. Int. J. Comput. Applic., 28: 10-17.

Bhattacharyya, D., T.H. Kim and S. Pal, 2010. A comparative study of wireless sensor networks and their routing protocols. Sensors, 10: 10506-10523.

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

Chen, H., 2009. Task-based Trust management for wireless sensor networks. Int. J. Secur. Applic., 3: 21-26.

Khalid, O., S.U. Khan, S.A. Madani, K. Hayat and M.I. Khan et al., 2013. Comparative study of trust and reputation systems for wireless sensor networks. Secur. Commun. Networks, 6: 669-688.

Lewis, F.L., 2004. Wireless sensor networks. Automation and Robotics Research Institute, The University of Texas at Arlington, Texas, USA., pp: 1-18.

Liu, S., L. Pang, Q. Pei, H. Ma and Q. Peng, 2009. Distributed event-triggered trust management for wireless sensor networks. Proceedings of the 5th International Conference on Information Assurance and Security, Volume 2, August 18-20, 2009, Xian, China, pp: 291-294.

Mahoney, G., W. Myrvold and G.C. Shoja, 2005. Generic reliability trust model. Proceedings of the 3rd Annual Conference on Privacy, Security and Trust, October 12-14, 2005, St. Andrews, New Brunswick, Canada, pp: 1-7.

Mariappan, E. and B. Paramasivan, 2015. Energy efficient cluster based transmission protocol in wireless sensor networks. Int. J. Soft Comput., 10: 169-174.

Michiardi, P. and R. Molva, 2002. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security, September 26-27, 2002, Portoroz, Slovenia, pp: 107-121.

Pandarinath, P., M. Shashi and A.A. Rao, 2010. A lightweight secure trust-based localization scheme for wireless sensor networks. Int. J. Comput. Sci. Inform. Secur., 8: 98-104.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, LA., pp: 90-100.

Rentala, P., R. Musunnuri, S. Gandham and U. Saxena, 2002. Survey on sensor networks. Technical Report UTDCS-33-02, University of Texas at Dallas, Dallas, TX., USA.

Tilak, S., N.B. Abu-Ghazaleh and W. Heinzelman, 2002. A taxonomy of wireless micro-sensor network models. Mobile Comput. Commuic. Rev., 6: 28-36.

Weatherall, J. and A. Jones, 2002. Ubiquitous networks and their applications. IEEE Wireless Commun., 9: 18-29.

Zahariadis, T., H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos and L. Besson, 2010a. Design and implementation of a trust-aware routing protocol for large WSNs. Int. J. Network Secur. Applic., 2: 52-68.

Zahariadis, T., H.C. Leligou, P. Trakadas and S. Voliotis, 2010b. Trust management in wireless sensor networks. Eur. Trans. Telecommun., 21: 386-395.