TFSR: trust factors evaluation-based secure routing protocol for wireless sensor network

V. Geetha*

Department of Information Technology,
National Institute of Technology Karnataka,
Surathkal, Karnataka, India
Email: geethav@nitk.edu.in
*Corresponding author

K. Chandrasekaran

Department of Computer Science and Engineering,
National Institute of Technology Karnataka,
Surathkal, Karnataka, India
Email: kch@nitk.ac.in

Abstract: Wireless sensor network (WSN) is an emerging technology, with tiny nodes to sense the data and collect it at sink node. The cryptographic techniques are not sufficient to ensure the security against blackhole, sink hole, DoS attacks, etc, as the nodes are deployed in open environment. Our main goal is to develop a trust-based secure communication system for WSN at network layer. We have identified various trust factors and developed a trust model for each trust factor to ensure security. We have proposed and analysed our trust factors evaluation-based secure routing (TFSR) protocol using network simulator NS2. The result shows that trust factors and trust models enhances secure communication in WSN for various possible attacks. The proposed model shows 96% of improvement, when alternative path for communication is available in the network. The result also shows total improvement of 30% to 35% in case of large networks.

Keywords: wireless sensor networks; WSNs; trust model; trust factor; blackhole; denial of service attack; ONOFF attack

Reference to this paper should be made as follows: Geetha, V. and Chandrasekaran, K. (2015) 'TFSR: trust factors evaluation-based secure routing protocol for wireless sensor network', *Int. J. Trust Management in Computing and Communications*, Vol. 3, No. 1, pp.40–73.

Biographical notes: V. Geetha obtained her Bachelor of Engineering degree from Mangalore University in 1999. She has obtained her MTech in Computer Science and Engineering from VTU, Belgaum in 2004 by securing 2nd rank. Currently, she is pursuing her PhD in Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal (NITK). She is also working as an Assistant Professor in the Department of Information Technology, NITK, Surathkal since from the year 2008. Her area of interest is computer architecture and wireless sensor networks. She has published total 20 papers in international journals and conferences.

K. Chandrasekaran is currently a Professor in the Department of Computer Science and Engineering, National Institute of Technology Karnataka. He is having 28 years of experience in teaching and research. His research interests include distributed computing, computer networks and cloud computing. He has more than 160 research publications in reputed or peer reviewed journals and international conferences. He is also a member in IEEE Computer Society's Cloud Computing Special Technical Community (STC). He was a Visiting Fellow/Researcher/Professor at various higher learning Institutes in India and abroad, which includes LMU UK, AIT Bankok and UF USA.

1 Introduction

In case of wireless sensor applications such as industrial monitoring, battlefield surveillance or disaster management systems, security of the network is one of the major concerns. Even though the cryptographic techniques can be used for secure communication, an adversary can still host various kinds of attack such as a blackhole attack, sink hole attack, DoS attack, etc. One of the solutions for identifying such attacks is to monitor the behaviour of sensor nodes (SNs) in the network. The behaviour monitoring helps to identify trustworthy and un-trust worthy nodes in the network. The behaviour of node can be monitored based on certain parameters relevant to application of wireless sensor network (WSN). Based on these factors the trust factors are evaluated periodically. The trust factors are used to identify various kinds of malicious nodes. Our approach is to provide a trust management mechanism which is ease to incorporate in any kind of WSN, and capable of identifying as many attacks as possible. There by the network can be kept safe in time critical WSN applications such as industrial monitoring, battlefield surveillance and disaster management.

WSNs provide a variety of applications in wireless technology. A large number of tiny SNs can be deployed in an environment to sense and send data to a base station called sink node (SK). The nodes are resource constraints, battery operated and self-configurable, which makes the WSN to have unique challenges about security. The traditional cryptographic techniques can provide the data confidentiality, data integrity and authentication. However, to overcome from DoS attacks, blackhole attack, selective forwarding attack, etc., one has to come up with more sophisticated techniques to identify such vulnerabilities in the network. Various trust models were proposed to detect and prevent such kinds of attacks. Most of the work considers one or two factors for calculating the trust values. For example, if the packet forwarding rate is considered as a factor for calculating trust, the attacks may still happen with the broadcast of packet (DoS attack) to drain the energy of nodes in the network. Therefore, identifying various factors which affect the trust among any two nodes is an important aspect. After identifying the various factors, it is also essential to evaluate each factor. Decision-making about malicious nodes based on the combined value of trust factor plays major role in identifying malicious nodes, which further reduces the chances of attacks on the network. Our work is to focus on answering the following questions related to trust factors.

1 What are the various factors which influence on trust between any two nodes in WSN?

2 How to evaluate each trust factor?

3 How to combine the trust factors to ensure trustworthiness of nodes in the network?

Trust is used in various domains like social network, P2P network, ad hoc network, etc., to build trust among two entities. In Section 2, we provide a survey on existing trust-based secure communication techniques. In Section 3, we identify various trust factors suitable for WSNs. In Section 4, we discuss about our proposed trust model for each trust factor. In Section 5, we show the simulation results for proposed trust factors evaluation-based secure routing (TFSR) protocol and discuss its relevance in identifying various kinds of attack. Section 6 concludes along with scope for future work followed by reference section.

2 Related work

This section discusses about trust factors represented in various domains of networks and evaluation methods. The trust between a boss and subordinates matters a lot in maintaining the healthiness of organisation NetForm (http://www.netform.com/html/s+b20article.pdf). The article NetForm (http://www.netform.com/html/s+b20article.pdf), explains about the behaviour of boss and subordinate in an organisation based on trust developed between employs. People in an organisation can be categorised as ‘hub’ or *workaholic*, who contributes in information flow, a ‘gatekeeper’, who has less knowledge and creates a bottleneck for information and the ‘pulse taker’ who shows their ability efficiently when the opportunity is provided. To develop trust between people in any organisation one of the factors that influences trust is the ‘response time’. If the response time is high, then the trust increases rapidly. The document IESE (http://www.iese.edu/en/files/irco-cross-cultural-corporate$_{t}cm$4–6121.pdf) mentions the factors which promote trust in organisations and among people. The personal factors and boss’s behaviour affect trust in the organisation. As personal factors are less changeable, trust mainly depends on the boss’s fit with the job. It indicates that following five types of behaviour by bosses foster trust in subordinates:

a consistency

b integrity

c communication

d delegation

e consideration.

Alam and Yasin (2010) identify various factors which influence online brand trust. Total nine website factors were identified, such as navigation, advice, no error, fulfilment, community, privacy/security, trust seals, brand and presence. These are the factors which influence on consumer’s trust. Along with these nine factors, the four consumer factors also effect on trust: self-confidence/internet savvy, past behaviour, internet shopping experience, and entertainment experience. The economic risk and performance risk also contributes to consumer trust.

Chen et al. (2008) provides trust factors in P2P networks. They classify the network as four types, namely, centralised, hierarchical, flat-based and one hop route-based networks. The trust factors are considered based on direct and indirect trust. In case of direct trust following factors are identified: requirement domain, service domain set, common transaction, specific transaction, feedback credibility, availability, time and risk. For indirect trust, following five factors were identified: common transaction, recommendation credibility, recommendation certificate, time, and risk. A general approach for evaluation is mentioned by specifying parameters for each metric. However, how to collect the values for each factor and in what way the evaluation has to be performed is not mentioned. The paper also mentions that designing a mathematical model for risk evaluation is still an open challenge.

Alhamad et al. (2011) provide trust evaluation metrics for cloud applications. Four factors are considered for evaluation of trust: scalability, availability, security, and usability. Fuzzy-based model is used to fuzzify each factor and evaluate the trust. This model is suitable for cloud applications as enough resources are available for computation and communication. Sun et al. (2005, 2006) propose an entropy-based model and probability-based model for ad hoc networks. In their proposed information theoretic framework, trust is a measure of uncertainty with its value represented by entropy. The experimental results show that malicious node detection is best in trust-based systems. Theodorakopoulos and Baras (2006) propose a trust model and evaluation metrics for ad hoc networks. Trust relations are based on evidence created by the previous interactions of entities within a protocol. In ad hoc networks, trust evidence may be uncertain and incomplete. The evaluation process is modelled as a path problem on a directed graph where nodes represent entities, and edges represent trust relations. The trusted path is considered for having better communication in the network. The trust and confidence levels are considered for evaluation of trust.

Feng et al. (2013) consider received packet rate, sending packet rate, packet forwarding rate, data consistency, time frequency, node availability and security grade (risk) as trust factors. Each factor is evaluated separately and direct trust evaluation is performed based on weighted average. To realise the fuzziness, subjectivity and uncertainty of trust evaluation, the D-S evidence theory is adopted to obtain the integrated trust value instead of the simple weighted average. However, the process of trust evaluation may need excess energy and time costs due to the increase in cooperation and communication with neighbours and the memory costs increases with the number of parameters, algorithm precision and network density.

Karkazis et al. (2011) propose a trust model which considers the factors such as packet forwarding, packet precision, network layer acknowledgment, authentication reputation response, reputation validation and remaining energy. The weighted average method is used to combine direct trust value. Hur et al. (2011) propose a trust evaluation model by considering identification, distance, sensing, communication, sensing result, consistency, battery and trust value as factors for trust. The main purpose is to provide data consistency based on location verification. Trust is calculated based on the weights provided for each factor. Hu et al. (2009) propose a weighted trust evaluation-based malicious node detection in WSNs. But, the aggregator nodes are considered as trustworthy nodes, practically which may not be the case. He et al. (2012) propose a distributed trust evaluation model and its application scenarios for medical sensor networks. Packet drop is considered as a factor and the beta-function-based method $T = (k + 1) / (N + 2)$ is modified as $T = \log_2(1 + ((k + 1) / (N + 2))$ where k is the number of successes and N is the total number of interactions. The equation uses logarithmic approach where it has a fast increase shape when the parameter is not a large number and a slow increase shape when the parameter is a large number.

Bao et al. (2012) propose a hierarchical trust management for WSN. The peer-to-peer trust evaluation process considers four different trust components: intimacy, honesty, energy and unselfishness by considering proper weights for each component. They propose an evaluation procedure for peer-to-peer, CH-to-SN, station-to-CH. It uses a probabilistic approach for calculating trust. The scheme achieves robust untrustworthy zone detection capability even if a majority of nodes in each zone is compromised.

Based on the related work, with respect to trust factors, we would like to summarise that following points must be considered in identifying the trust factors in WSN.

1 Identifying trust factors for WSN is more important.

2 The method for evaluation of each trust factors need to be developed for identifying various malicious behaviour of nodes in the network.

3 A WSN needs a robust trust model to ensure secure communication with various trust factors.

3 Identifying trust factors for WSN

The first step in developing a trust management system for WSN is to identify necessary trust factors. In this section, we identify various trust factors and discuss their relevance in evaluation of trust in WSN.

3.1 Trust definition and characteristics

Yu et al. (2012) define trust for WSNs as “trust is a subjective opinion in the reliability of other entities or functions, including the veracity of data, connectivity path, processing capability of the node and availability of service, etc.” Since the definition given by Yu et al. (2012) provides a way for defining trust with various factors, we consider the same definition for our work. Following are the basic characteristics of trust in WSNs.

1 Trust is subjective: The trust value of a node *j* observed by another node *i* depends on the observed behaviour of the node *j* with respect to perspective of node *i*.

2 Trust is dynamic: If the node *i* trusts node *j* with respect to some aspect, it does not guarantee that node *j* also trusts node *i* with equal trust value.

3 Trust is non-transitive: If a node *i* trusts node *j* and node *j* trusts another node *k*, then, it does not ensure that node *i* also trusts node *k*.

4 Trust is reflexive: The node *i* trusts itself.

5 Trust is context sensitive: The node *i* trusts node *j* for some specific operation. This characteristic indicates, trust on one context is different from some other context.

Trust value can be represented by the range of values between [0, 1]. The value 0 represents complete untrustworthiness and the value 1 represents complete trustworthiness. The range of values represents likeliness of trustworthiness. Trust definition is same across various trust factors.

3.2 Assumptions

Following are our assumptions for developing a method for evaluation of trust factors.

1 Each SN uses cryptographic mechanism to ensure data integrity, confidentiality and authorisation.

2 The nodes are static and synchronised with time.

3 SNs are deployed densely enough to sense some identical events redundantly with their own neighbour nodes.

3.3 Identifying trust factors

SNs can build trust based on various factors. We mainly classify these factors into seven categories.

1 communication trust

2 data trust

3 trust based on functionality of node

4 location trust

5 energy trust

6 trust update time

7 risk.

The relevance of each trust factor in WSNs is explained in detail in following subsections.

3.3.1 Communication

The communication in WSN mainly involves the packet transfer from one node to another node in the network. The factor of the rate at which each node transfer the packet, contributes towards evaluation of trust. Packet transfer can be further classified into five sub factors:

1 *Packet send*: The node senses the data and sends packet to SK.

2 *Packet receive*: The node receives the packet sent by a base station or other cluster head (CH) node requesting for information. The received query packets can be considered as the packets received (PR).

3 *Packet forward*: Some nodes act as intermediate nodes in the network, which forwards the packet towards SK.

4 *Broadcast packet*: The nodes in the network may generate the broadcast packet to share common information. An attacker can simply generate the broadcast packet to flood the network with packets and drain the energy of nodes. To monitor on such action in the network, the rate at which broadcast packets were sent must be monitored.

5 *Control packet*: The packets exchanged for routing or other control operations.

3.3.2 Data trust

The major functionality of WSN is to collect information from the environment, as a result, data is one of the factors which influences on trust. This factor can be further classified into four sub-components: consistency, integrity, confidentiality and aggregation. The first three components can be ensured by checking with the cryptographic technique used in the system. The data aggregation must deal with attacks such as stealthy attack where a node simply sends data value which is very high or low compared to neighbour nodes sensed values, so that the aggregation value gets impacted at cluster level. We classify the trust factor for data into two major categories:

1 *Data security*: The factor which contains consistency, integrity and confidentiality as subfactors.

2 *Data aggregation*: The factor which deals with the stealthiness of data at the CH level.

3.3.3 Functionality of node

Bao et al. (2012) consider the functionality of node as one of the factors for evaluation of trust value. It is true that in WSN all the nodes do not play the same role in functionality. So the functionality of nodes is also one of the factors which contributes to the trust in WSN. Based on functionality we can classify the nodes as SN, cluster node, and SK. The confidence in each node can be calculated based on previous history of nodes behaviour with respect to its functionality. In case of hierarchical networks, the CH must consider the functionality of SN as well as SK. The SN must consider the functionality of CH. Similarly, the SK must consider the functionality of CH as a factor for trust calculation.

3.3.4 Location trust

The location of a node can be identified in two ways.

1 based on hop count/region

2 based on the GPS system.

The malicious node may provide incorrect information for the nodes about their location in order to mis-route or gather the information from all nodes in the network. As a result, ensuring the correctness of location is a factor in building trust among nodes.

3.3.5 Energy

The SNs are resource constraint in terms of memory, computation and communication energy as the nodes are battery operated. The malicious nodes may try to drain the energy of nodes in the network. As a result, energy is one of the trust factor in WSN.

3.3.6 Trust update time

The WSN is deployed to sense critical information in an environment. In such environment, the trust update time is one of the major factor. On a trust value, following two components of time impacts:

1. *Trust calculation time*: The trust calculation time can be fixed as static for the network with periodic data update. The trust update time can be kept as dynamic for aperiodic or event-based data transfer network.
2. *Nodes response time*: Response time is one of the major factor which influences on the trust. If there is a high response from the neighbour, then the trust value must be increased, as the node is providing good response for communication.

3.3.7 Risk

In case of WSN, until a certain amount of communication takes place initially, the behaviour of neighbour nodes is uncertain. At this point of time, a node considers ‘risk’ as a factor to evaluate and decide about further possible communications with the neighbour nodes.

Table 1 Trust factors and possible attacks related to vulnerabilities in WSNs

Sl. no.	*Trust factor*	*Parameters*	*Type of attack which can be detected based on trust factor*
1	Communication trust	PS, PF, PR, PB, PC	Sink hole or blackhole attack, Hello flooding attack, Selective Forwarding (Grey hole) attack, Node replication attack, Acknowledgement Spoofing, DoS attack
2	Data trust	Data security, data aggregation	Stealthy attack
3	Functionality trust	Sink, CH, SN	Sink hole or blackhole attack, Hello flooding attack, Selective Forwarding (Grey hole) attack, Node replication attack, Acknowledgement Spoofing, DoS attack.
4	Location trust	Location	Sybil attack (Node Replication attack)
5	Energy trust	Availability	DoS attacks related to energy
6	Trust update time	Communication, data	Effects trust value, which further relates to communication trust and data trust
7	Risk	Communication, data	Support for communication and data trust

The trust factors are identified in WSN for evaluating trust in WSN. Table 1 lists the trust factors and associated sub factors, using which various types of attacks can be detected in the network. A trust model is required to evaluate each trust factor. Finally, the trust values of each trust factor must be combined to evaluate and to identify total trustworthiness of each node in the network. A node may cooperate for communication trust, but it may try to host stealthy attack. A node may cooperate for communication and data trust, but it may try to become the CH as often as possible, and may not send data to SK. The combined evaluation of trust factors must be able to detect the malicious activity of a node with respect to each trust factor.

4 Proposed trust model for evaluation of each identified trust factors

We have identified total seven trust factors which influence trust in WSN. They are:

1 communication trust

2 data trust

3 functionality of trust

4 location trust

5 energy

6 trust update time

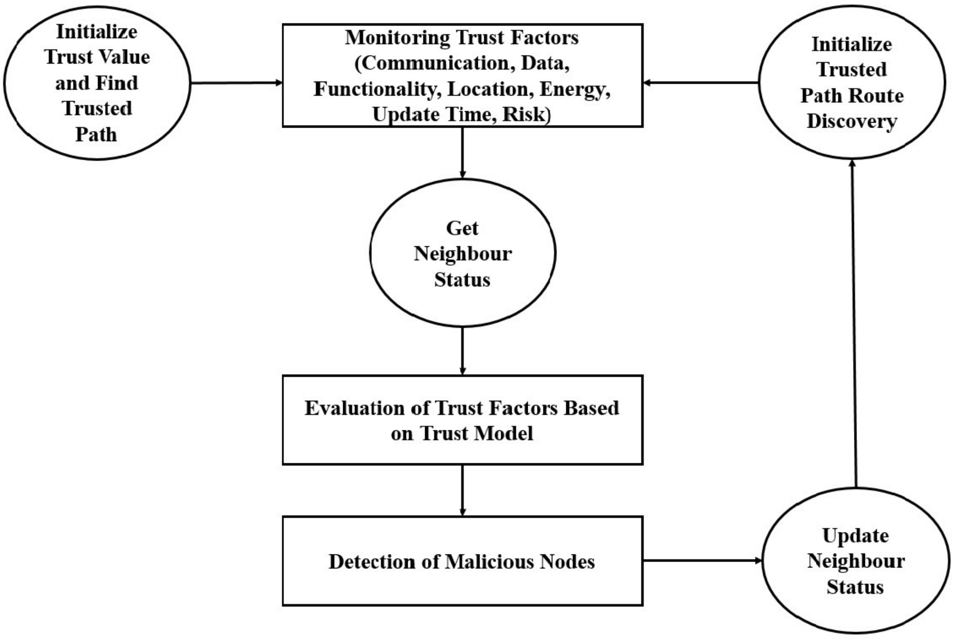
7 risk.

This section describes the trust model for each identified trust factor.

Trust modelling is nothing but a mathematical representation of a node's opinion of another node in a network. That is, we need mathematical tools to represent trust, and update it continuously based on new observations and finally make the decision about the trustworthiness of nodes in WSNs. Several probability distributions can be used to represent the trust of a node, such as beta, Gaussian, Poisson, binomial, etc., as they have a sound theoretical foundation and deal with uncertainty problems. The beta distribution is used to represent when transactions are binary. We use beta distribution and Bayesian estimation to classify nodes as misbehaving or normal nodes. Ganeriwal and Srivastava (2004) provide a beta distribution and Bayesian estimation-based trust model. We consider the same for modelling trust in WSN with necessary modifications for identifying various kinds of attacks. Normally, indirect trust is useful in dynamic topologies like ad hoc networks, to converge the trust values as early as possible. As the nodes of WSNs are static in nature for most of the application, we consider that, the analysis on direct observation-based trust is more sufficient for calculation of trustworthiness.

Figure 1 shows the working of TFSR protocol. Initially, all the nodes assume that, the nodes in the network are trustworthy and starts communication. For each interaction, the trust factors are monitored. For every interval of trust update time, each node gets trust factor values and evaluates it based on a trust model proposed in Sections 4.1 to 4.7. If nodes are identified as malicious nodes, then trust values are updated accordingly and new trusted route discovery process is initiated.

Figure 1 TFSR: TFSR protocol for WSN


Initialize Trust Value and Find Trusted Path
Monitoring Trust Factors (Communication, Data, Functionality, Location, Energy, Update Time, Risk)
Initialize Trusted Path Route Discovery
Get Neighbour Status
Evaluation of Trust Factors Based on Trust Model
Detection of Malicious Nodes
Update Neighbour Status

4.1 Trust model for communication trust

Based on Ganeriwal and Srivastava (2004) trust model, it can be identified that, the probability of succession can be obtained by Bayesian inference, by observing on two parameters α and β. The expected value can be obtained as α / (α + β) according to Baye's and (α + 1) / (α + β + 2) according to Laplace law, which considers that at least one 'success' and one 'failure' were observed before observing *n* trials where $n = (\alpha + \beta)$. A node will observe a neighbouring node's behaviour and build a trust for that node based on the observed information. The neighbouring node's transactions are direct observations referred as firsthand information. For each observation, the node *i* maintains two parameters α and β which indicates the number of 'successful' and 'unsuccessful' operation by a neighbour node *j*.

$$T_{ij} = (\alpha + 1) / (\alpha + \beta + 2) \tag{1}$$

The communication trust denoted as T_{ij}, is initialised to 0.5 based on Laplace Law. The Trust is calculated as shown in equation (1) where α_j and β_j represents the number of 'successful' and 'unsuccessful' cooperation by node *j* to node *I*, respectively. As the SNs are resource constraint, maintaining the history of all observed trials is resource consuming. To solve this issue, the α_j and β_j are updated periodically, based on *r* and *s* where *r* indicates number of 'successes' and s indicates number of 'unsuccessful' cooperation in a time window *t*.

$$\alpha_j = \alpha_j + r \text{ and } \beta_j = \beta_j + s \tag{2}$$

Then α_j and β_j can be updated as shown in equation (2).

$$\alpha_j = W_{age} * \alpha_j + r \text{ and } \beta_j = W_{age} * \beta_j + s \text{ where } 0 <= W_{age} <= 1. \tag{3}$$

As the data becomes old, the oldest information has to be discarded to provide a higher preference for latest information. Ganeriwal and Srivastava (2004) provide the concept of aging factor, W_{age} to update α_j and β_j as shown in equation (3). Since it provides high weightage for past interactions, a node can perform ONOFF attack very easily. A ONOFF attack is one where a node behaves benevolent until it obtains a high trust value with good history of records, and then starts dropping packets (ON) and forwarding packets (OFF) periodically. As a result, the nodes can launch attacks, even while maintaining its trustworthiness. To overcome such attacks, the proposed punishment-based technique in Geetha and Chandrasekaran (2013) is used for detecting ONOFF attack.

We consider that the communication trust related to packet transfer is one of the major functionality in WSN. As a result, the weighted average method is used for calculating trust for each type of packet transfer. The trust between node *i* and node *j*, where node *i* is an observer of behaviour of node *j*, related to communication can be denoted as $T_{Communication}$. This is a function of the number of packets sent (PS), PR, packets forwarded (PF), broadcast packets received (PB) and control packets received (PC).

$$TotalPacketTransfer = PS + PR + PF + PB + PC; \tag{4}$$

$$\begin{aligned} WeightedTrust = {} & (W_{PS} * PS) + (W_{PR} * PR) + (W_{PF} \ * PF) \\ & +(W_{PB} * PB) + (W_{PC} * PC); \end{aligned} \tag{5}$$

$$TCommunication = WeightedTrust \,/\, TotalPacketTransfer; \tag{6}$$

where

$$W_{PS} + W_{PR} + W_{PF} + W_{PB} + W_{PC} = 1. \tag{7}$$

The *TCommunication* is calculated according to the equation (4) to (7). Initially, the network does not contain any prior information about its neighbour. As a result, equal weights such as 1/5 can be considered as weight to calculate communication trust. We propose that, as the interaction with the neighbour node increases, the weights can be calculated based on the ratio of packet transfer with respect to sub operations like PS, PR, etc. to the total number of interactions performed with respect to corresponding neighbour node. This helps to clearly distinguish roles of SNs such as leaf nodes, data forwarding node, etc. The weights for each sub component of communication trust can be updated for every interval of trust update time as follows:

W_{PS} ratio of PS to total number of packets

W_{PR} ratio of packet received in total number of packets

W_{PF} ratio of packet forwarded to total number of packets

W_{PB} ratio of packet forwarded to total number of packets

W_{PC} ratio of control PS/received in total number of packets.

4.2 Trust model for data trust

We propose that data trust can be calculated by considering *data security* and *data aggregation* components. *TDataSecurity*: The data security component depends on the cryptographic technique used in the network. If the technique is robust to provide data security, then more weight can be given for data aggregation. *TDataaggregation*: The data is aggregated normally at CH. If the application is sensitive about data aggregation, then more weightage can be given for (1 – α) as shown in equation (8).

$$TData = \alpha * TDataSecurity + (1-\alpha) * TDataAggregation \tag{8}$$

where $0 <= \alpha <= 1$.

The data Trust denoted as *TData* is calculated as in equation (8). The data trust is initially introduced by Momani and Challa (2007) by considering the Gaussian distribution for calculating the trust with normal distribution. The idea is to check the variance of the node data with respect to data sensed by receiving node, over a period of time. Each node is assessed with respect to its own sensed data over a period of time. To converge the value, second hand information is used. The area under cumulative probability distribution function (CDF) from ($-e$, e) is considered as the trust value. We would like to mention here that the $\phi(x)$ calculation in normal distribution is having computational complexity. The wireless SNs are very limited with resources. Hence, we propose following method for calculating data trust. A SN i receives data from various SNs which are connected to it, for sending its sensed data. Let N nodes are connected to SN j where $j = 1, 2, 3, \ldots, N$ and $j \neq i$. The SN i waits for collecting the data from all j nodes represented as x_j, aggregates the data and forward it to SK. If data aggregation is done with simple average, there are chances that a node with a stealthy attack can send the data with very high or low value to effect on aggregated data value. Same thing gets applied in case of min() and max() functions. The challenges in data aggregation are as follows:

1 selecting the data which are normal at a selected point of time t

2 selecting data from only trusted nodes for data aggregation.

Selecting data in normal range: We propose that standard deviation can be used to calculate the lower and upper bound range for normalising the data. Let x_i be the data collected from all nodes, including its own sensed data.

$$Mean(\mu) = \left(\sum_1^N x_i\right) \Big/ N \text{ and } Variance\left(\sigma^2\right) = \left(\sum_1^N x_i - \mu\right) \Big/ N \tag{9}$$

The mean of the data is calculated as shown in equation (9). The ($\mu - \sigma$) and ($\mu + \sigma$) provides the lower and upper bound of data, respectively. The data within the range of upper and lower bound is considered as valid data. The range of data can be selected based on the type of application.

Trust of the node based on data: The data of node within the range of ($\mu - \sigma$) and ($\mu + \sigma$) can be considered as a 'successful' operation and the data not within this range, is considered as 'unsuccessful' operation. Now the problem is similar to calculation of communication trust. Hence, we use the trust model explained in Section 4.1 as the model for data trust. The data trust is calculated as $DataTij = (\alpha + 1) / (\alpha + \beta + 2)$ where α_j and β_j represents the number of 'successful' and 'unsuccessful' data access from node *j* to node *i*. As the SNs are a resource constraint, maintaining the history of all observed trials is resource consuming. To solve this issue, the α_j and β_j are updated periodically, based on *r* and *s* where *r* indicates number of ‘successes’ and s indicates number of ‘unsuccessful’ cooperation in a time window *t*. The α_j and β_j can be updated as based on equation (2). As the data becomes old, the oldest information has to be discarded to provide a higher preference for latest information. Ganeriwal and Srivastava (2004) provide the concept of aging factor, W_{age} to update α_j and β_j as in equation (3).

Table 2 Algorithm for evaluation of functionality trust

```
Function Functionalitytrust= calculateftrust(ctrust,dtrust)
Constant CThresh, DThresh
// Threshold values for communication trust and data trust
if Communicationtrust ≥ CThreshandDatatrust ≥ DThresh
    Functionalitytrust = (Communicationtrust + Datatrust) / 2.0;
elseif Communicationtrust < CThreshandDatatrust < DThresh
    if (Communicationtrust < Datatrust)
        Functionalitytrust = Communicationtrust;
    else
        Functionalitytrust = Datatrust;
    end
elseif Communicationtrust < CThreshjjDatatrust < DThresh
    if (Communicationtrust > Datatrust)
        Functionalitytrust = Communicationtrust;
    else
        Functionalitytrust = Datatrust;
    end
end
```

4.3 Trust model for functionality trust

WSN contains three different types of nodes based on their functions. SN which senses and sends the data, CH which performs aggregation and sends data to SK and SK which collects all packets and monitors overall operations in the network.

The algorithm for calculating functionality trust of a SN, based on its communication trust and data trust is shown in Table 2. The SK can similarly calculate the trust of CH based on its functionality. In this case, only communication trust plays the role as the CH sends aggregated data to SK. We assume SK is trustworthy with respect to functionality.

4.4 Trust model for location trust

The location information given by a neighbour node can be checked based on received signal strength. If distance calculated from the received location information from neighbour and distance calculated through received signal strength are same, then location information can be considered as trustworthy information.

4.5 Trust model for energy trust

Energy is one of the important factor which influences on trust. If a node is having less energy, and if it is not able to communicate with any node, then the node is in the stage of exhausting its energy and it's not a malicious node. A node can be checked for its energy level, based on which its trust value can be calculated. For example, if a node is having higher energy and if it is still not sending any packet continuously, then it indicates node is a malicious node. The energy level can be calculated based on two techniques.

1 Explicitly receiving energy information from each node

2 Calculate energy of neighbour node based on received signal strength.

$$\text{EnergyTrust} = \text{Ccapacity}/\text{Tcapacity} \tag{10}$$

$$\text{Ccapacity} = \text{CremainingEnergy} / \text{EnergyTotransmitOnePacket} \tag{11}$$

$$\text{Tcapacity} = \text{IEnergy} / \text{EnergyTotransmitOnePacket} \tag{12}$$

Trust based on energy value is calculated based on equation shown in 10, where Ccapacity indicates current capacity, which is the number of packets the node can still send based on its current energy and Tcapacity indicates total capacity, which is the total number of packets a node can send with its initial energy (IEnergy). The Ccapacity and Tcapacity are calculated based on equations (11) and (12). The node can calculate the energy in terms of ability to send number of packets in future.

4.6 Model for trust update time

The time at which the trust for a node is calculated also matters a lot in trust calculation. If the trust is updated frequently, then it increases computation for every round of trust calculation. If trust is updated less frequently, then chances are there that the malicious nodes take advantage of it. So the challenge is finding answers to the question, 'What must be the trust update time interval?'. In a WSN, we can observe that the nodes are sending data either periodically, or based on emergency of the event. We would like to consider packet rate as the parameter to calculate the update time. Let packet rate per unit time be $P_t/unit$ time. If the packet transfer rate is increased per unit time, then reduce the trust update time. If the packet rate is normal, then update the trust at previously calculated interval of time. Consider, for example, packet rate per hour is calculated as $Packets = TotalPacketsPerDay \ / \ 24$. If the number of packets to be sent per hour is reached earlier than an hour, then calculate trust else calculate trust per every hour. Another way to view the trust update time is to update the trust for every packet received. But to have energy efficiency the trust update value can be fixed based on number of tolerable drop of packets in the network. If the application is more critical and sensitive, then update the trust for each packet, otherwise, set the trust update interval for number of tolerable packet drops. This factor can also be used as a factor for W_{age} in communication trust calculation.

4.7 Trust model for risk

The risk factor has to be considered if no previous information about the neighbour node is available. Based on the parameters, if communication trust and data trust are available then risk is less. Otherwise the risk factor gets attached to all other trust factors. Coming up with a model for risk calculation is a crucial task. We propose a method for calculating the Trust on risk. TRisk is calculated as complement of ratio of number of interaction up to current time (*t*) to Total possible interactions.

$$\text{TRisk} = \left(1 - (\#\text{InteractionsCurrentTime}) / (\text{Total possible interactions})\right) \tag{13}$$

The trust based on risk is calculated as shown in equation (13). Total possible interaction is calculated based on initial energy and average transmission time per packet. A node *i* tries to check whether it has sufficient history of interactions with the node *j*. As the number of interactions increases the value of factor Risk decreases.

4.8 Combining trust values of each trust factor

The complete trustworthiness of a node depends on evaluation of each trust factor and combined trust value of the same. Even though the trust factors may rely on various assumptions, environment, setup, etc., still trust values of trust factor can be combined, as all the trust values are represented in the range of [0, 1], where 0 represents ‘no trust’ and ‘1’ represents complete trustworthiness and any other value between 0 and 1 represents likeliness of trustworthiness. The trust factors must be evaluated or combined to calculate the total trust of a node based on communication factor, data aggregation, functionality, and location. The trust value of risk and energy plays an important role in combining trust values. We propose a new way of combining trust values based on energy and other trust factors.

$$TotalComm = CT * WC + DT * WD + FT * WF + LT * WL \tag{14}$$

Since communication, data, functionality and location are related to interactions with respect information exchange, we propose a weighted average technique to combine trust values of these factors. The total communication trust *TotalComm* is calculated as shown in equation (14), where CT is communication trust, DT is data trust, FT is functionality trust and LT is location trust.

If communication trust is low, then automatically data trust and functionality trust cannot be given with full weight. If the nodes are static in the network, then number of times the location trust calculated is very minimum. The relation of weights can be considered as WC >> WD, WF, WL. We know that, WC + WD + WF + WL = 1. As a result, an ideal weight for each one can be considered with the ratio 4:2:2:2, respectively.

The final trust value of a node based on all the trust factors, denoted as *FinalTrust* is calculated based on algorithm shown in Table 3. This combined trust value provides a way for evaluating the trust of a node based on various kinds of trust factor. Final trust calculation can be used to identify the next set of CHs for forthcoming rounds, or to find full trust worthy nodes in the network for secure routing. A CH can try to identify the fully trusted nodes in its region, thereby assigning higher and sensitive tasks to trust worthy node.

Table 3 Algorithm for evaluation of functionality trust

```
$Totaltrust = TotalComm * (1 - TRisk)$;
if $EnergyTrust >= EThresh$
    $FinalTrust = Totaltrust$;
else
    $FinalTrust = EnergyTrust$;
end
```

5 Simulation results and discussions

The simulation is carried out in network simulator (NS2, http://www.isi.edu/nsnam/ns/), to verify the trust model. The simulation on NS2 is performed with IEEE 802.15.4-based SNs. Our proposed protocol is compared with ad hoc on demand distance vector (AODV) routing protocol. In case of the proposed TFSR protocol, each SN calculates the trust for its neighbour node based on its neighbour behaviour. Watchdog technique is used to find the number of packets successfully forwarded by its neighbour. The node also keeps track of the number of broadcast PS, number of PB, number of control PS and number of PC to calculate communication trust. The data trust is always kept as high value as the nodes are not having any clusters to aggregate the data. So the question of stealthiness does not arrive at SNs in TFSR. Energy and location trust are calculated based on periodic HELLO packet information exchange. The path trust is calculated based on the trust of nodes in that particular path. Each node while sending its route request (RREQ), it also sends the value of ratio of number of trustworthy nodes in its neighbourhood. The SK sends route reply to a path which is having highest trustworthy nodes among all the paths. Simulation is carried out by considering two different topologies.

1. with two routes for SK
2. more generalised random topology.

5.1 Attacker model

The simulation results are analysed for blackhole, DoS and ONOFF attack. For simulation, the attacker model is considered as follows:

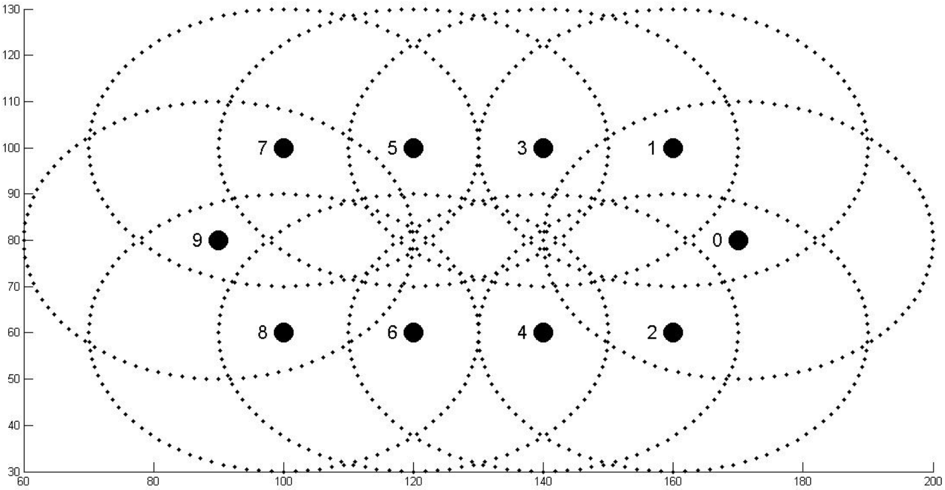
1. Blackhole attack: When a node '*i*' is set as a blackhole attacker, the node receives the PS/forwarded by its neighbour and node '*i*' simply drops the packet without forwarding it towards SK.
2. Denial of service attack: When a node '*i*' is set as DoS attacker, the node '*i*' frequently sends a number of RREQ packets to initiate broadcast attack, so that the nodes in the network get exhausted because of RREQ flooding. RREQ with a new sequence number, initiates flooding in the network.
3. ONOFF attack: When a node '*i*' is set as ONOFF attacker, the node acts as benevolent until it achieves high trust value (0.9). After obtaining a high trust value, the node starts dropping the packet for a period of time (ON) or until the trust value

is above a threshold value (0.5). After reaching lower threshold value, the node again starts behaving benevolent for a period of time (OFF) or until it reaches a high trust value (0.9). This cycle of ON and OFF continues throughout the simulation. The node '*i*' approximately calculates the trust value by keeping an account on its interaction with neighbour nodes.

5.2 Simulation results and discussions for two path topology

The topology considered for our simulation is shown in Figure 2. The node 0 is SK. The nodes 1, 3, 5, and 7 are not reachable to node numbers 2, 4, 6, and 8 as their communication range are not reachable. Node 9 is between nodes 7 and 8. Hence, we have two different paths to reach SK from the node 7. The main idea of choosing this topology is to check the route change process and its effect on control packets in the network. Initially, the network uses the shortest path for communication. When a node detects, its neighbour as malicious node, then the route to sink gets changed based on the trustworthy nodes, by selecting a trusted path which may or may not be the shortest path. For simulation, we have considered the scenario, where node 7 sends the data to SK periodically. During normal operation, the sink chooses the path as 7->5->3->1->0. If any node in this path detects any kind of malicious nodes, then the SK chooses the second path 7->9->8->6->4->2->0 based on trust on this path. We have compared AODV and proposed TFSR for blackhole, DoS and ONOFF attacks.

Figure 2 Topology of WSN



The simulations are run with scenarios for no attackers, one attacker and two attackers. The results are analysed based on following metrics.

1 Packet delivery fraction (pdf): The ratio of data PR by the destinations to those generated by the source node.

2 Normalised routing overhead (nrl): The number of routing packets transmitted per data packet delivered at the destination.

2 Total number of RREQ PS

4 Total number of RREQ PR

5 Life time of the network: Life time of the source node until it exhaust with the energy or it does not have any route, whichever is earlier.

5.2.1 Analysis of blackhole attack

The effectiveness of communication trust is tested against blackhole attack. The blackhole attack is one, where the attacker drops the packet without forwarding it towards SK. The node 7 starts sending packets periodically to SK.

The node 3 and node 4 are kept as blackhole attacker and results are taken for scenario with no attacker, one attacker node, two attacker nodes. The DoS attack is initiated at 50 second at node 3 and node 4. Figure 3, 4, 5, 6, and 7 show the results of simulations.

Figure 3 shows that the *pdf* is equal to 1 in case of AODV and TFSR with No attacker. In case of one attacker in one path, the blackhole attacker in AODV drops all the packets, and the network is not able to detect it. However, in proposed TFSR, since trust-based routing is incorporated, the node which identifies the blackhole attacker, results in changing the route with trusted path. This results in *pdf* with value 1 for TFSR. When both paths in network topology contain blackhole attacker, both AODV and TFSR performs poorly, as there is no trusted path left out for further communication. TFSR maintains high *pdf*, until it has some trusted routing path towards SK.

Figure 3 Packet delivery fraction for blackhole attack

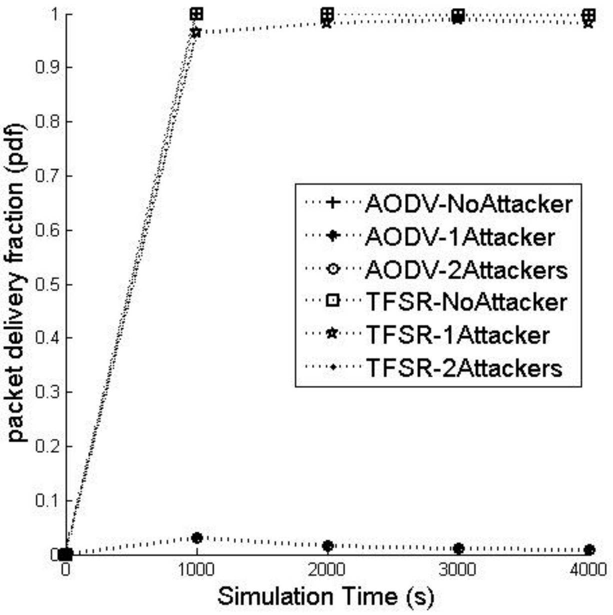


Figure 4 Network routing load (nrl) for blackhole attack

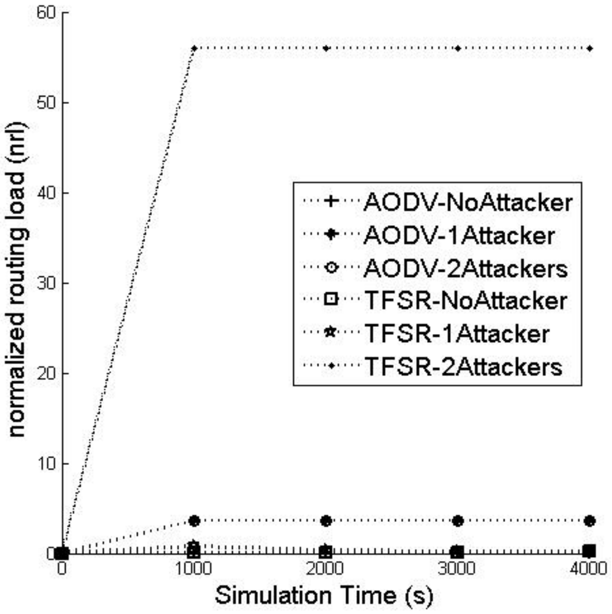


Figure 5 Number of RREQ PS in the network

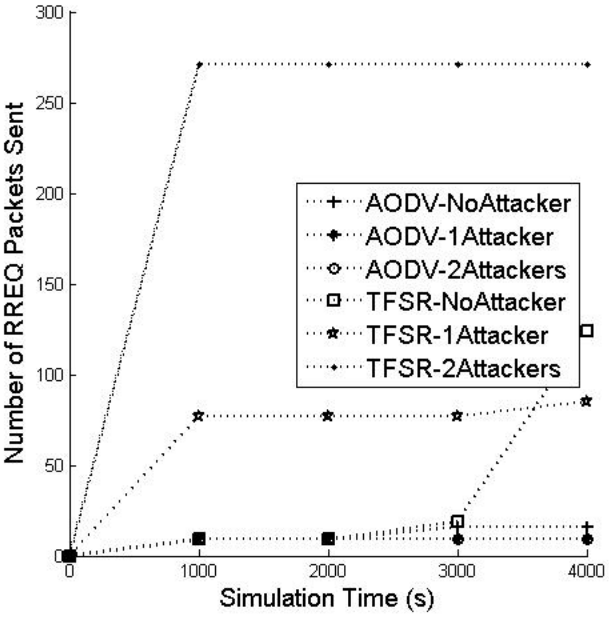


Figure 6 Number of RREQ PR in the network

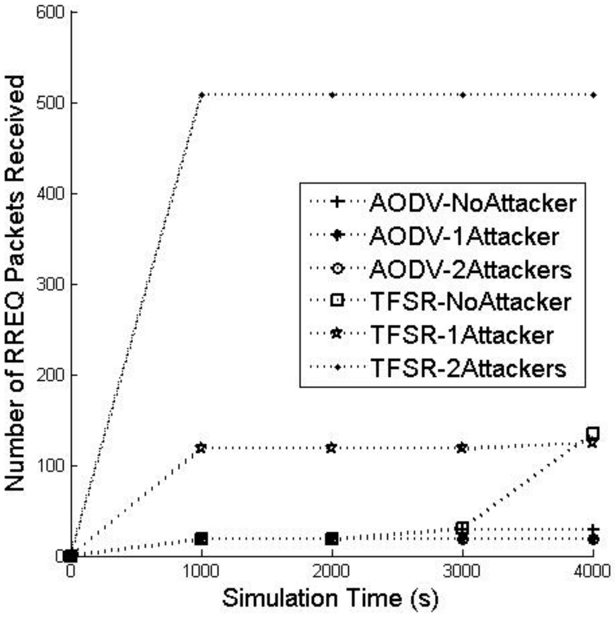


Figure 7 Life time of network for blackhole attack

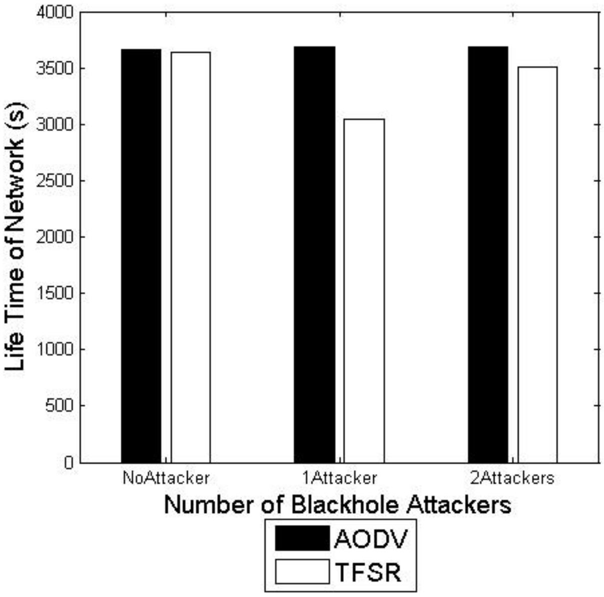


Figure 8 Packet delivery fraction for DoS attack

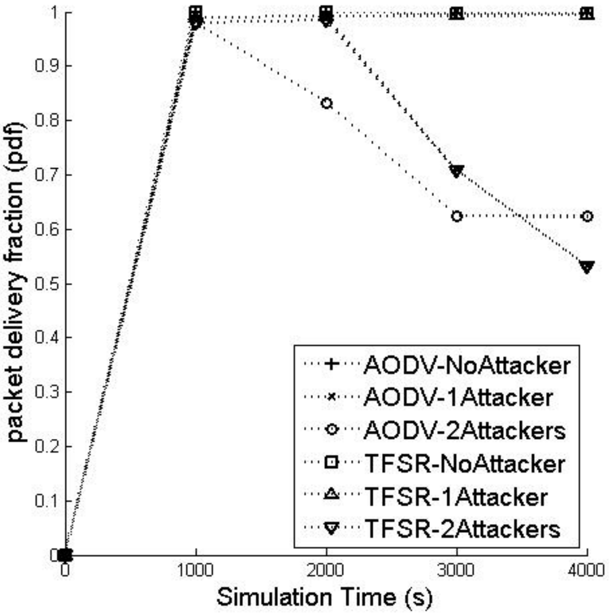


Figure 4 shows the results for normalised routing load (nrl). The *nrl* for AODV in case of No attacker, one attacker, two attackers is low compared to TFSR. Since the AODV does not detect any malicious node and incorporates any route change, the number of control PS per packet is less. The *nrl* for TFSR for one attacker is almost equal to the *nrl* with No attacker. This shows that if there is a trusted path existing, the change of route does not increase *nrl* in the network. The *nrl* for attackers in both the path, increases *nrl* for TFSR and AODV, since there is no trusted path. Most of the time will be spent in finding a trusted path and due to a blackhole attacker no packets get transmitted to SK.

Figure 5 shows the cumulative results for the number of RREQ PS in the network with respect to simulation time. The Number of RREQ PS is more for TFSR compared to AODV. However, as TFSR finds a trusted path, it provides better *pdf*.

Figure 6 shows the cumulative results for the number of RREQ PR in the network with respect to simulation time. The Number of RREQ PR is more for TFSR compared to AODV. However, as TFSR finds a trusted path, it provides better *pdf*.

Figure 7 shows that the lifetime of AODV and TFSR are almost same for AODV and proposed TFSR in case of no attackers. The lifetime of the network is more for AODV in case of one attacker, as most of the packets are not getting transferred. The TFSR has less lifetime compared to AODV. But, the *pdf* is 1 for TFSR and almost 0 for AODV in case of one attacker. In case of attackers in both the paths, AODV and TFSR behaves almost same.

In summary, in the presence of blackhole attack, the TFSR performs compared to AODV, as TFSR chooses more trusted path. Hence, packet delivery will be more compared to AODV. As TFSR is able to detect blackhole attack provides *pdf* with high value until it has a trusted path to SK.

5.2.2 Analysis of DoS attacks based on broadcast packet trust

Denial of service attacks (DoS) attacks is one of the major issues in WSN as it tries to drain the energy of nodes in the network. In case of AODV routing protocol, a node can frequently send a number of RREQ packets to initiate broadcast attack, so that the nodes in the network get exhausted because of RREQ flooding. The trust-based monitoring helps to identify DoS attacks and reduce the effect of it over the network. The DoS attack is initiated at 50 second at node 5 and node 6. Figures 8, 9, 10, 11, and 12 show the results of simulations.

Figure 8 shows that the packet delivery fraction is 1 for AODV with no attacker, TFSR with No attacker and TFSR with one attacker. The value of *pdf* decreases as the simulation time increases. The DoS attack in AODV reduces the *pdf* as it creates flooding of control packets and drains the energy of a node. We can observe that when there is a trusted path, TFSR chooses trusted path and hence the *pdf* value is equal to 1.

Figure 9 shows the *nrl* values with respect to simulation time. The normalised routing overhead zero for AODV and TFSR when there is no attack. The *nrl* for TFSR is less compared to AODV in case of one attacker and two attackers. As it is a DoS attack, the number of control packets are more in the network. However, TFSR handles a DoS attack by not forwarding the control packets, if a node is identified as malicious with respect to DoS attacks.

Figure 9 Network routing load (nrl) for DoS attack

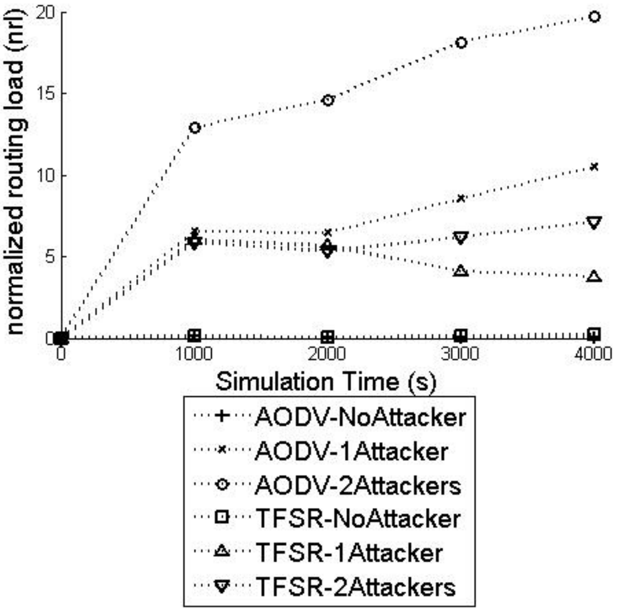


Figure 10 shows the result for a number of RREQ PS on the network. It clearly shows that the number of RREQ sent packets is more for AODV and less for TFSR in the presence of DoS attacks. Since the node which detects DoS attacks stops forwarding RREQ from that particular node, it reduces the number of broadcasts. The same is reflected in Figure 11. Figure 12 shows the lifetime of network in case of DoS attacks.

The lifetime is same for AODV and TFSR for network with no attackers. The lifetime of AODV is less for TFSR, as the nodes in the network dies due to broadcast of DoS attack packets.

Figure 10 Number of RREQ PS in the network

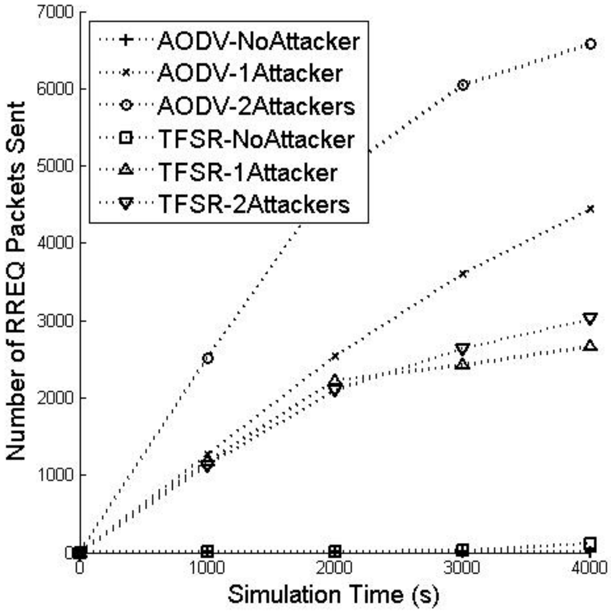


Figure 11 Number of RREQ PR in the network

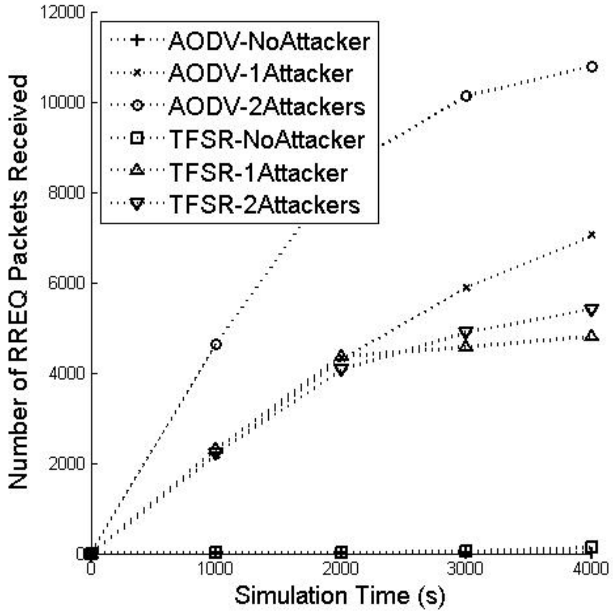
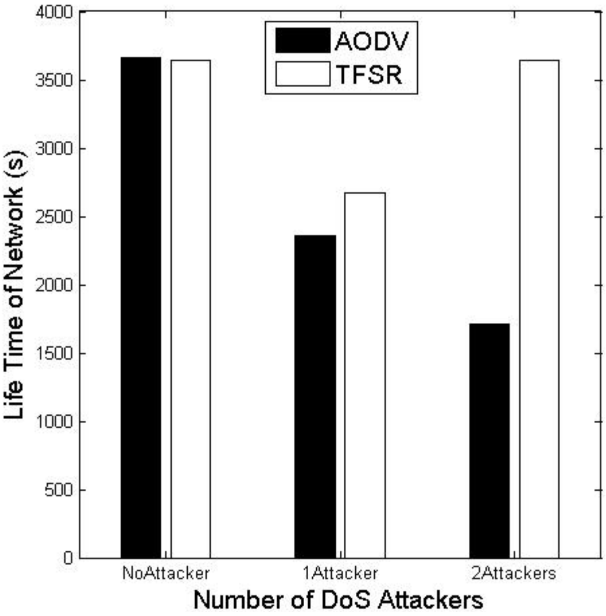


Figure 12 Life time of network for DoS attack



In summary, the TFSR detects DoS attacks and improves on *nrl* compared to AODV. The TFSR works better until there is a trusted path to SK.

5.2.3 Analysis of ONOFF attacks

One of the attacks possible with the trust-based system is ONOFF attack, where a node initially waits for obtaining high history and then starts dropping the packet for a period of time (ON) and again starts behaving benevolent for a period of time (OFF). Identifying such attack is very essential in case of WSN, where the WSN is used for some critical applications. For simulation, the ONOFF attack is initiated at 1,000 second at node 3 for one attacker. Node 3 and 4 are ONOFF attackers for two attacker simulation. Figures 13, 14, 15, 16, and 17 show the results of simulations.

Figure 13 shows the results for *pdf* for AODV and TFSR with ONOFF attackers. With ONOFF attacker, the *pdf* with no attacker and with one attacker is 1 in case of TFSR. The *pdf* value decreases in the presence of attackers with AODV. The results show that, the TFSR *pdf* is more for one attacker compared to AODV with one attacker. But, *pdf* reduces for Two attackers, as the attacker is present in both the paths.

Figure 14 shows the values *nrl* with respect to simulation time. The *nrl* value of AODV and TFSR are zero and same with no attackers. The *nrl* value increases less compared to AODV in the presence of one ONOFF attacker. The *nrl* value increases in the case of two attackers as there is no trusted path to transfer the data.

The number of RREQ PS and received is shown in Figures 15 and 16, respectively. The results show that the control packet transfer AODV is more compared to TFSR.

Figure 17 shows the lifetime of network for AODV and TFSR protocols. The lifetime of AODV is less compared to TFSR as the number of control packets increases in AODV.

Figure 13 Packet delivery fraction for ONOFF attack

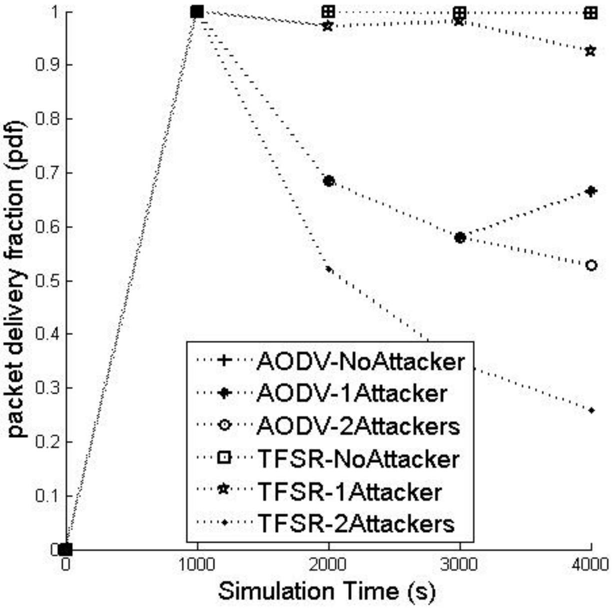
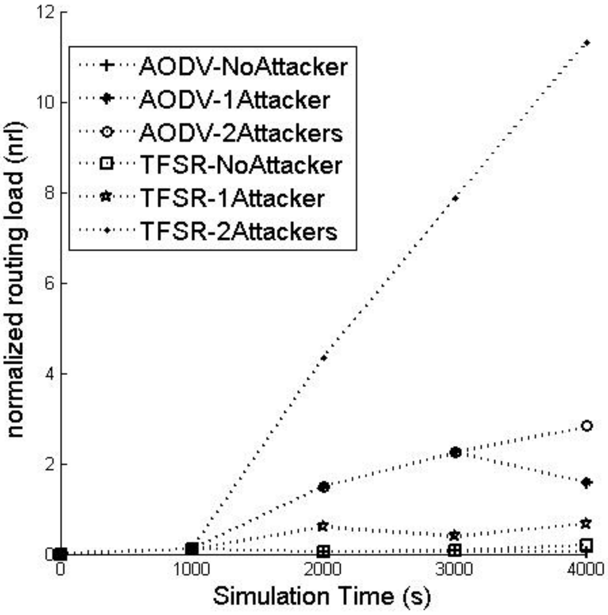


Figure 14 Network routing load (nrl) for ONOFF attack



In summary, the TFSR is able to detect ONOFF attack and hence its *pdf* increases compared to AODV.

Even though in this paper, we have shown the results for three types of attacks. The results show that the packet delivery in network improves by 96% in the presence of alternative path towards a destination compared to the routing protocols without trust management systems. We ensure that the monitoring on proposed trust factor can be used for other similar kind of attacks in WSN.

Figure 15 Number of RREQ PS in the network

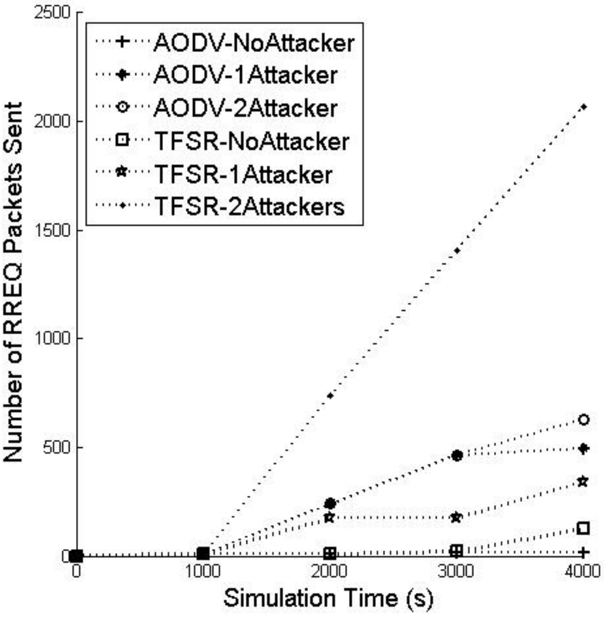


Figure 16 Number of RREQ PR in the network

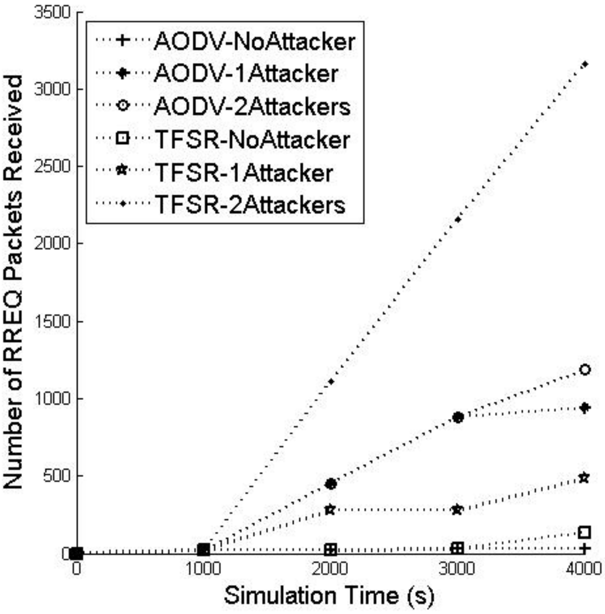
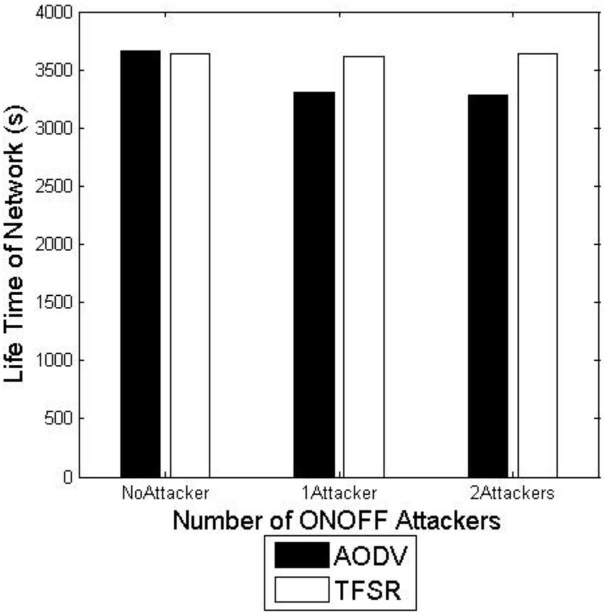


Figure 17 Life time of network for ONOFF attack



5.3 Analysis of results for random topology

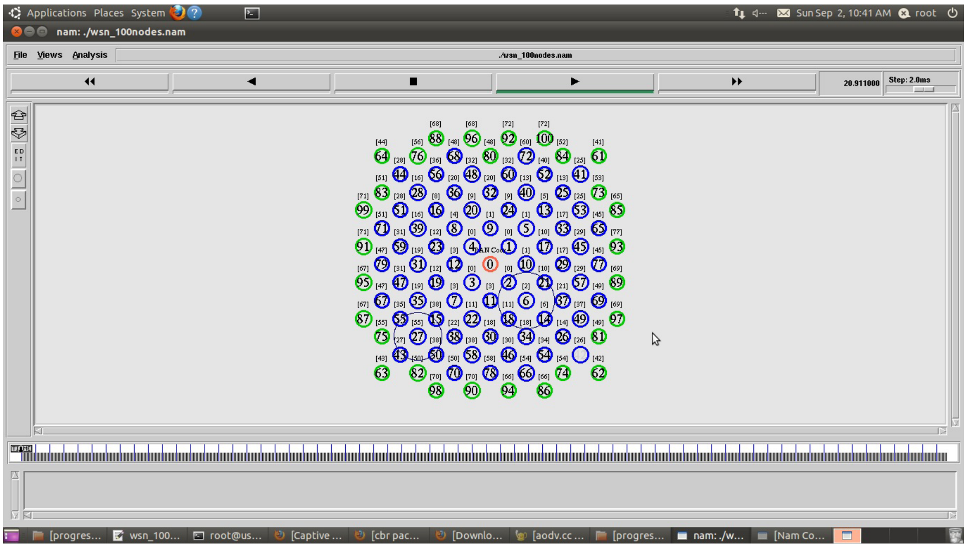
The simulation is carried out for random topology and results are compared with directed diffusion (DD) routing. DD and AODV are reactive protocols. DD is a data-centric algorithm for collecting information from the network. Base station flood interests for named data, setting up gradients within the network designed to draw events. Nodes which are able to satisfy the interest disseminate information along the reverse path of interest propagation.

Table 4 Simulation parameters for random topology

Simulation parameters	*Value*
Simulation time	86,400 sec (24 hours)
Topology size	100 × 100 m^2
Number of nodes	101
BS position	Center of the network
Radio propagation model	Two ray ground
Antenna model	Antenna/Omniantenna
PHY and MAC layer	IEEE 802.15.4
MAC	Beacon enabled/peer-to-peer
Monitoring time	2,000 seconds
Traffic type	Constant bit rate (CBR)
CBR rate	1 packet/200 seconds

Each node is monitored based on the successful and unsuccessful cooperation for data forwarding operation by neighbouring nodes. Trust for each node is calculated at a specified interval of time in order to reduce the computation cost of updating trust values for each packet forwarding. The network contains one SK, and the nodes generate traffic for sending data which can be viewed as sensing of data and forwarding at a specified interval of time. Simulations are carried out in order to observe the behaviour of nodes in the network by monitoring the interactions and to identify the malicious nodes based on threshold values. The topology of the network is as shown in Figure 18. Based on the trust of observed node the corresponding path trust is evaluated to eliminate the attackers. The results of TFSR are compared with AODV and DD algorithm. Details of the simulation environment are mentioned in Table 4. The results are analysed for *pdf*, and *nrl* for AODV, TFSR and DD protocols.

Figure 18 Topology of network considered for simulation (see online version for colours)



5.3.1 Analysis of blackhole attack

Figures 19 and 20 show the results of packet delivery fraction and normalised routing load for AODV, TFSR and DD with no attackers and with 30% attackers in the network. It clearly shows that, the pdf for AODV, TFSR and DD is high and good while no attackers are present in the network.

However, the *pdf* fraction of AODV is low compared to DD and TFSR, when 30% nodes are blackhole attackers in the network. The normalised routing load increases when there are attacker nodes in the network. The *nrl* is high for TFSR compared to AODV and DD as there are routing packet overhead to identify the alternate path in case of TFSR.

Figure 19 Packet delivery ratio for blackhole attack

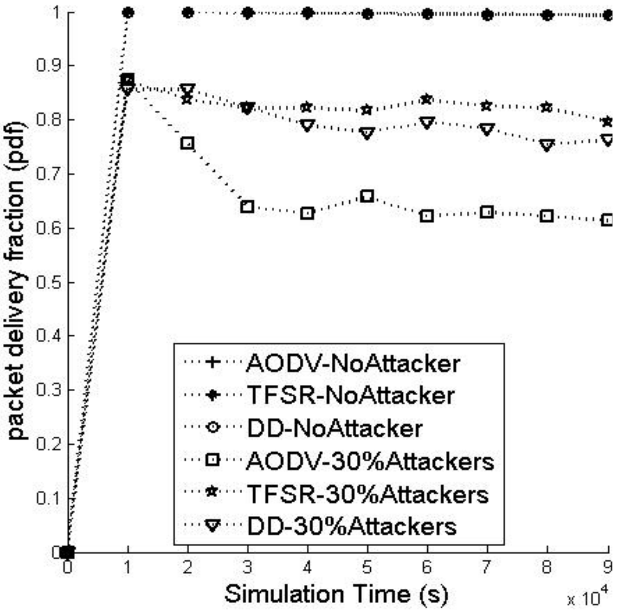


Figure 20 Normalised routing load for blackhole attack

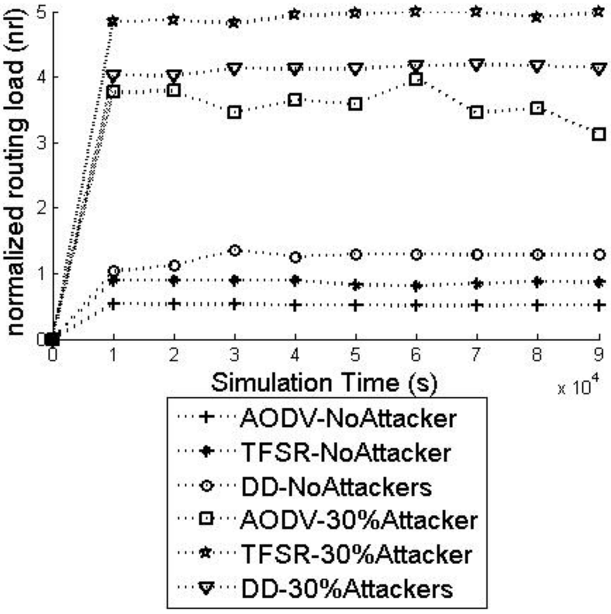


Figure 21 Packet delivery ratio for DoS attack

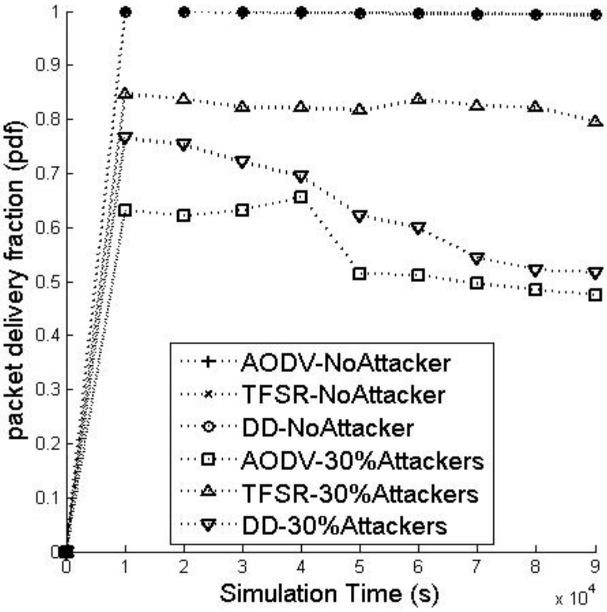


Figure 22 Normalised routing load for DoS attack

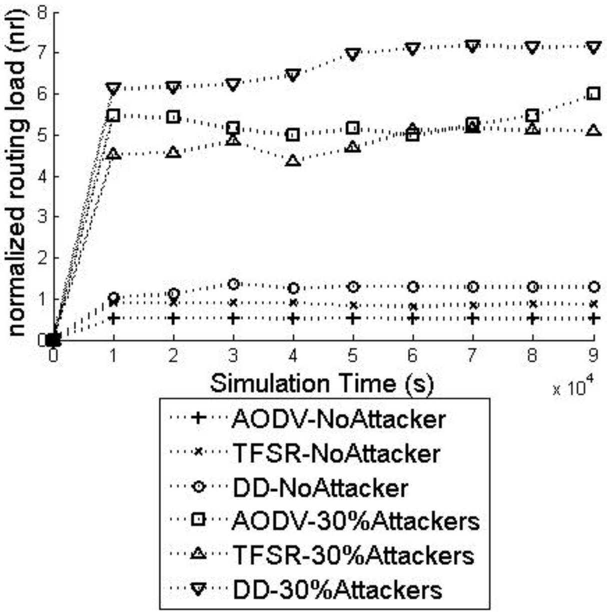


Figure 23 Packet delivery ratio for ONOFF attack

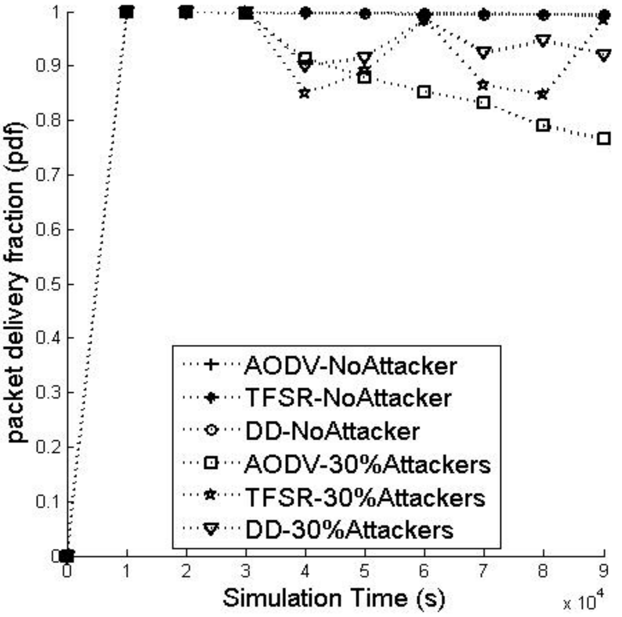
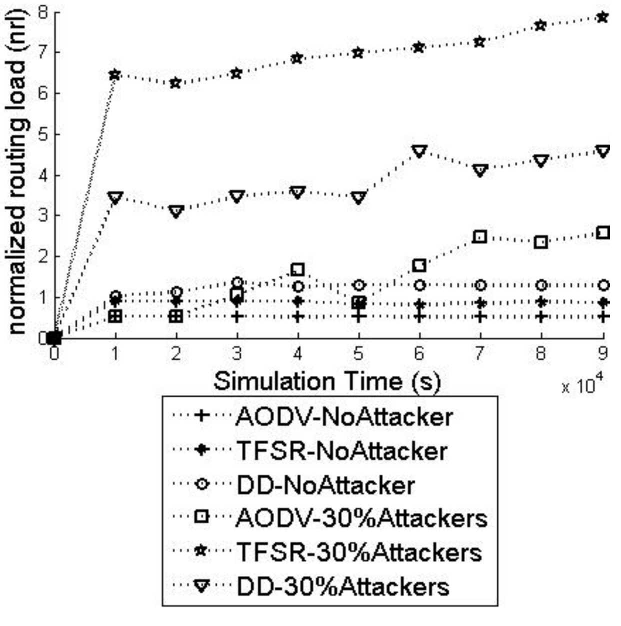


Figure 24 Normalised routing load for ONOFF attack



5.3.2 Analysis of DoS attack

Figures 21 and 22 show the results for packet delivery ratio and normalised routing load for AODV, TFSR and DD routing protocols, with no attackers and 30% DoS attackers present in the network. Figure 21 shows that the packet delivery ratio is high and almost equal to one when no attackers are present in the network. In the presence of DoS attack, the packet delivery ratio decreases in cases of AODV and DD protocol. The TFSR performs better compared to AODV and DD as the nodes take corrective measure against DoS attacks. Figure 22 shows that normalised routing load for TFSR more compared to AODV and DD as the TFSR sends re-initiates path discovery after identifying DoS attack.

5.3.3 Analysis of ONOFF attack

Figures 23 and 24 show the packet delivery ratio and normalised routing overhead for AODV, TFSR and DD routing protocols with no attacker and 30% ONOFF attacker. Figure 23 shows that the *pdf* variation for ONOFF attack is more in case of AODV compared to other two protocols. Figure 24 shows that the *nrl* for TFSR is high compared to AODV and DD as the nodes initiates the process of route discovery by sending appropriate control messages, after identifying any malicious node.

5.4 Results and discussions

The simulation experiments are carried out on two kinds of topology.

1 a topology with only nine nodes and two paths to SK

2 a topology with large number of nodes, i.e., 100 nodes with one SK, with alternate paths available for SK.

The results are compared for blackhole, DoS and ONOFF attacks. The results are also analysed for AODV, DD and TFSR protocols. The TFSR provides a better solution for blackhole attack, DoS attack as well as ONOFF attack with increase in *nrl*. Its a trade-off between security and *nrl* in the network based on the application.

6 Conclusions

The trust-based routing protocols are essential for identifying various kinds of attack such as blackhole attack, DoS attacks, ONOFF attack, etc. It is essential to identify various trust factors required to be monitored to analyse the behaviour of nodes in the network. In this paper, we have identified various trust factors which influence on trust in WSN. The trust factor is evaluated based on various parameters observed on the network. The relevance of each factor and its associated parameters are discussed. The trust factors identified in the WSN need to be evaluated to find trustworthiness of the nodes. We have proposed a trust model for various trust factors. The simulation results are analysed for blackhole, DoS and ONOFF attacks in the network for AODV, TFSR and DD protocols. The results show that TFSR performs better compared to AODV and DD until there exists a trusted path towards the destination. The proposed trust evaluation method can be extended for any routing protocol based on trust factors. We conclude that, trust monitoring on various trust factors and its evaluation is necessary for detecting different kinds of attack on the network. This is an ongoing work, and in future we would like to analyse the model for various other kinds of attack for further improvements.

References

Alam, S.S. and Yasin, N.M. (2010) 'What factors influence online brand trust: evidence from online tickets buyers in Malaysia', *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 5, No. 3, pp.78–89.

Alhamad, M., Dillon, T. and Chang, E. (2011) 'A trust-evaluation metric for cloud application', *International Journal of Machine Learning and Computing*, Vol. 1, No. 4, pp.416–421.

Bao, F., Chen, I-R., Cahng, M. and Cho, J-H. (2012) 'hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection', *IEEE Transactions on Network and Service Management*, Vol. 9, No. 2, pp.169–183.

Chen, H., Chen, G., Liu, J., Luo, X., Li, X. and Li, B. (2008) 'Trust factors in P2P networks', *Proc. of IEEE International workshop on semantic Computing and Systems*, pp.49–54.

Feng, R., Che, S., Wang, X. and Yu, N. (2013) 'Trust management scheme based on D-S evidence theory for wireless sensor networks', *International Journal of Distributed Sensor Networks*, Article ID 948641, 9pp, doi:10.1155/2013/948641.

Ganeriwal, S. and Srivastava, M.B. (2004) 'Reputation-based framework for high integrity sensor networks', *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington DC, USA.

Geetha, V. and Chandrasekaran, K. (2013) 'Enhanced beta trust model for identifying insider attacks in wireless sensor networks', *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 13, No. 8, pp 14–19.

He, D., Chen, C., Chan, S., Bu, J. and Vasilakos, A.V. (2012) 'A distributed trust evaluation model and its application scenarios for medical sensor networks', *IEEE transactions on Information Technology in Biomedicine*, Vol. 16, No. 6, pp.1164–1175.

Hu, H., Chen, Y., Ku, W-S., Su, Z. and Chen, C-H.J. (2009) 'Weighted trust evaluation-based malicious node detection for wireless sensor networks', *International Journal on Information and Computer Security*, Vol. 3, No. 2, pp.132–148.

Hur, J., Lee, Y., Yoon, H., Choi, D. and Jin, S. (2005) 'Trust evaluation model for wireless sensor networks', *Proc. of the 7th International Conference on Advanced Communication Technology, ICACT 2005*, pp.419–496.

IESE [online] http://www.iese.edu/en/files/IRCO-Cross-cultural-Corporate_tcm4-6121.pdf (accessed March 2015).

Karkazis, P., Ventouri, A., Voliotis, S., Zahariadis, T., Leligou, H.C. and Trakadas, P. (2011) 'Configuring trust models for WSNs', *18th International Conference on Systems, Signals and Image Processing, IWSSIP 2011*.

Momani, M. and Challa, S. (2007) 'GTRSSN: Gaussian trust and reputation system for sensor networks', in Sobh, T.M. (Ed.): *SCSS (1)*, pp.343–347, Springer.

Quantum Theory of Trust [online] http://www.netform.com/html/s+b%20article.pdf (accessed March 2015).

Sun, Y., Yu, W., Han, Z. and Liu, K.J.R. (2005) 'Trust modeling and evaluation in ad hoc networks', *Proc. of Global Telecommunications Conference, GLOBECOM '05 IEEE*, pp.1862–1867.

Sun, Y.L., Yu, W., Han, Z. and Liu, K.J.R. (2006) 'Information theoretic framework of trust modeling and evaluation for ad hoc networks', *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp.305–317.

The Network Simulator (NS2) [online] http://www.isi.edu/nsnam/ns/ (accessed June 2014).

Theodorakopoulos, G. and Baras, J.S. (2006) 'On trust models and trust evaluation metrics for ad hoc networks', *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp.318–328.

Yu, Y., Li, K., Zhou, W. and Li, P. (2012) 'Trust mechanisms in wireless sensor networks: attack analysis and countermeasures', *Journal of Network and Computer Applications*, Vol. 35, No. 3, pp.867–880.