Wireless Sensor Network, 2014, 6, 173-183
Published Online September 2014 in SciRes. http://www.scirp.org/journal/wsn
http://dx.doi.org/10.4236/wsn.2014.69017

Scientific Research

A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network

Geetha V.[1], K. Chandrasekaran[2]

[1]Department of Information Technology, National Institute of Technology, Karnataka, Surathkal, Karnataka, India
[2]Department of Computer Science and Engineering, National Institute of Technology, Karnataka, Surathkal, Karnataka, India
Email: geethav@nitk.edu.in, kch@nitk.ac.in

Received 23 June 2014; revised 22 July 2014; accepted 21 August 2014

Abstract

The wireless sensor network is an emerging technology, which is used to sense and monitor the environment. As the nodes are deployed in an open environment, the security is one of the essential factors. The cryptography techniques can ensure confidentiality, integrity and authentication. However, wireless sensor network also needs to deal with inside and outside attackers. To deal with outside attackers, attacks by compromised or malicious nodes, trust management system is suggested by many researchers in the area of wireless sensor network. Trust management system can be implemented in various applications for security management such as secure data aggregation, secure cluster head selection, trusted routing, access control, etc. Many researchers provide different kind of solutions for these secure applications based on trust management. However, to incorporate, all such applications on a single sensor node in the network, it is essential to design and develop a trust management system, which considers various aspects and applications of wireless sensor network. As a result, in this paper, we would like to propose a parameter and trust factor based secure communication framework and design a trust management system for wireless sensor networks. Our main contribution is to identify various parameters and trust factors which influences on trust in wireless sensor network and developing a framework for a trust management system based on various parameters and trust factors. The working of the proposed model is shown by simulation experiments conducted in MATLAB for the application of secure communication, data aggregation and intrusion detection in wireless sensor networks.

Keywords

Wireless Sensor Network, Trust Management System, Black Hole, Sinkhole, DOS, Trust Factors

How to cite this paper: Geetha V. and K. Chandrasekaran (2014) A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network. *Wireless Sensor Network*, **6**, 173-183. http://dx.doi.org/10.4236/wsn.2014.69017

1. Introduction

The Wireless Sensor Network (WSN) is an emerging technology where a number of tiny nodes are deployed in an open environment to sense various phenomena [1]. As the sensor nodes are resource constraint and are deployed in an open environment, the nodes are more prone to inside and outside attacks. Cryptography technique can ensure authentication, confidentiality and integrity. However, to deal with outside attacks such as black holes, sink hole, Denial of Service (DOS) attacks, researchers propose a trust based system. Trust management has proven good results in other network areas such as social networks, ad hoc networks and P2P networks. The trust models and methods which are applicable to other networks are not directly applicable to wireless sensor network, as WSN is a resource constraint network.

Trust in WSN can be viewed as communication trust and data trust or node trust, path trust and service trust. The following definition of trust provides general factors needs to be addressed in wireless sensor network.

"*Trust is a subjective opinion on the reliability of the other entities or functions, including veracity of the other data, connectivity path, processing capability of the node and availability of service etc.*"

The trust is subjective, non-transitive, reflexive and asymmetric in characteristics. The trust between node increases if the node performs every action according to the specific rules of networking. If a node violates the rules of the network, then the nodes must be identified as malicious nodes and further eliminate these nodes from further communication in the network. The node can build the trust based on its direct observation and recommendation. The recommendation, trust ensures convergence of trust values faster based on neighbor recommendations. However, these recommendation systems are more helpful, when the topology of nodes changes dynamically. The exchange of recommendation information in secure way increases communication cost. As a result, it is better to use direct observation based trust for calculating the trust of a node in the network.

Belief is the probability of a node that decides the level of trust. For example, 0 indicates complete distrust and 1 indicates complete trust. The expected probability of belief is trust and actual probability is said to be trustworthy. Miscalculation of trust and trustworthiness difference will leave scope for poor risk estimation over vulnerabilities. In some cases, trust alone is not sufficient in all operations. However, risk, quality of service and trust need to be dealt separately before they are included in the trust computation.

Many researchers propose trust model and trust management system for one particular layer of the network protocol stack. But, the trust management system must deal with various kinds of application in each layer of the protocol stack. Most of the time, the trust management system considers very few parameters and trust factors for evaluation of trust. A trust management framework must consider various parameters and trust factors associated with building trust among nodes in wireless sensor network.

In trust management system, each sensor node must observe its neighbor based on various parameters such as packets forwarded, broadcast packets, etc. Based on these observed parameters the trust factors are evaluated. The combined value of these trust factors ensures the trustworthiness of a neighbor node. The framework proposed in this paper considers these aspects in developing a trust management system.

The main questions to be addressed are: How best does the trust model detect malicious nodes? How best does it take action on detection of malicious nodes? What is the rate of false positive and false negative? What is its impact on wireless sensor network? etc. In this paper, we propose a framework for trust based secure communication in wireless sensor network. The rest of the paper is organized as follows: Section 2 discusses about related work in the area of trust based framework proposed for various kinds of network. Section 3 presents our proposed trust based secure communication framework for wireless sensor network. Section 4 discusses about simulation results and discussion, followed by conclusions and reference.

2. Related Work

The researchers proposed various frameworks for trust based secure communication for different kinds of networks such as a social network, ad hoc network, p2p network and wireless sensor networks. Farruh Ishmanov *et al.*, [2] provides a detailed insight on the trust management system in wireless sensor networks. They have discussed about the importance of trust management in wireless sensor network as well as compared various kinds of trust models. They have also listed various open research issues such as monitoring and learning, trust evaluation, trust propagation, attack resistance and performance comparison of trust management systems. Since, wireless sensor network itself is an emerging area, the trust system for wireless sensor network is still new which needs further improvement in various aspects. As a result, the trust management system essentially has a

major role in providing secure communication. Fenye *et al.*, [3] proposes a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks to effectively deal with selfish or malicious nodes. The trust is evaluated based on multiple attributes. Ganeriwal *et al.* [4] Proposed reputation based framework for data integrity in wireless sensor networks. The proposed reputation system takes information collected by each node using a watchdog mechanism to detect invalid data and uncooperative nodes. Yao *et al.* [5] proposed a parameterized and localized trust management scheme for WSN security, particularly for secure routing, where each node maintains a highly abstracted parameter to evaluate its neighbors. Junqi Duan *et al.* [6] provides a framework for trust aware secure routing. They have given a framework for considering a trust model for routing protocol. Javier Lopez *et al.*, [7] provides a list of best practices for developing a good trust management system for wireless sensor network. Chen *et al.*, [8] provides an event based trust management framework model. The trust is calculated based on event occurs and confidence. Most of the trust model focus on one type of application of trust management systems. It is essential to provide a framework, where the trust management system is considered across various layers of the protocol stack and which is applicable for detecting various kinds of attacks.

3. Proposed Trust Based Secure Communication Framework for Wireless Sensor Network

Secure communication is one of the essential factors in wireless sensor network as the nodes are deployed in an open environment. Each node in the network, must be capable of identifying malicious nodes, securely aggregate the data, identify trustworthy nodes in its neighbor, and cooperate for all the activities of the network with its group. We propose, a parameter and trust factor based trust management system for wireless sensor network. The system design of the trust management system is shown in **Figure 1**.

The trust management system is not a single layer in the protocol stack of wireless sensor network. We propose that the trust management system must be designed across the layers, as the security has to be ensured in all layers of wireless sensor network. As a result, the protocol stack, Application, Transport, Network, Data link and Physical layer, interacts with the trust management system as shown in **Figure 1**.

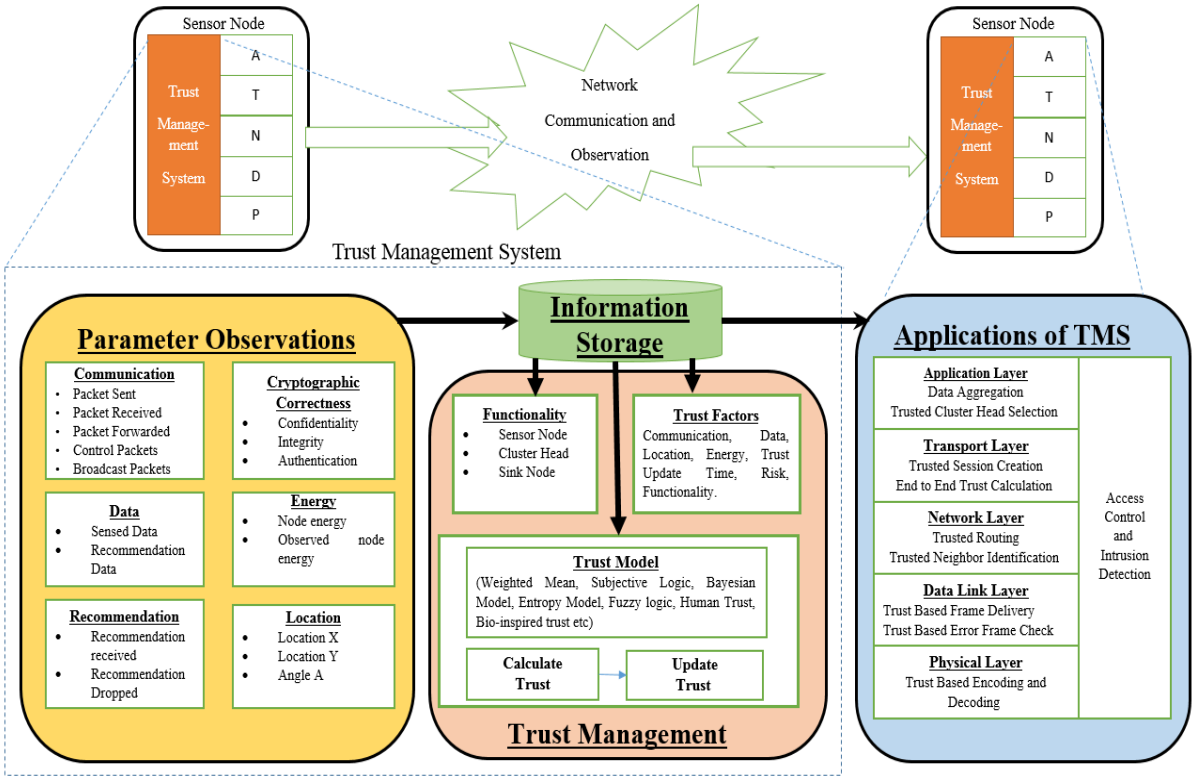

Figure 1. Proposed trust management system for wireless sensor networks.

Node A can communicate to Node B over the wireless media. Each event is observed in the network for developing trust on neighbor nodes. The proposed trust management system, mainly consider following components.

- Parameter Observation
- Trust Management
- Information Storage and
- Trust Applications

Each component is discussed in detail in following subsections.

3.1. Parameter Observation

To calculate trust between two nodes, a node *i* has to observe its neighbor *j* for its interactions with node *i*. Every event *e* is observed on the network. We have identified total six groups of data to be observed on the network. They are Communication, Data, Recommendation, Location, Energy, and Cryptographic Correctness.

- Communication: The node *i* observes node *j* for all the events related to communication. The parameters associated with *communication* are as follows: Number of packets sent (PS), Number of packets received (PR), Number of packets forwarded (PF), number of control packets sent (PCS), number of control packets received (PCR) and number of broadcast packets received (PB), number of data packets sent (PDS), number of data packets received (PDR).
- Data: The data of sensor node contain two parts. Either a node has to store its own sensed data or the data which it has forward towards sink node. The sensor node can sense static data or multimedia data. The information about data has to be stored for further processing. If the trust management uses indirect trust, then, the recommendation sent by neighbor nodes can also be treated as data.
- Recommendation: The number of recommendation packets sent and received also helps to monitor, the neighbor node with respect to the node behavior in sending recommendations.
- Location: In most of the routing protocols, the protocol considers geographical location based routing. A node may lie on its location information. To monitor such events, a node can request location information of node *j*, either from node *j* itself or node *i* can find out based on node *j*'s received signal strength.
- Energy: Energy is one of the essential aspect of wireless sensor network, as the nodes are resource constraint.
- Cryptographic correctness: This parameter is used to check, whether a node in the network is behaving properly according to cryptographic rules.

3.2. Trust Factors

The trust of a neighbor node is calculated based on evaluation of trust factors. Each trust factor is evaluated based on observed parameters. We have identified seven trust factors which mainly influence on trust of a node. Each trust factor is a function of a set of parameters.

- **Communication Trust:** This communication trust factor is a function of parameters observed for communication behavior. The communication trust factor is evaluated based on parameters as follows:

  ***Communication Trust* (*PS, PR, PF, PCS, PCR, PB, PDS, PDR*);**

  The communication trust factor may consider weighted average technique to evaluate all parameter values to communication trust value.

- **Data Trust:** The trust factor data is used to calculate trustworthiness with respect to data in the network. Attacks such as the stealthy attack can effect on the data aggregation. Similarly, in case of recommendation based trust calculation, the verification of recommendation data is also essential. As a result, the trust factor data contains two subcomponents: *Sensed data* and *Recommendation data*. The trust factor *Data Trust* is evaluated based on these two parameters as follows:

  ***Data Trust* (*Sensed Data, Recommendation Data*);**

  The data trust can provide certain weights for *sensed data* and *recommendation data*. If recommendation system is not used, then only *sensed data* information can be used to calculate Data Trust.

- Functionality Trust: Based on topology the wireless sensor network can be classified as flat based network or hierarchical based network. For flat based network topology, the nodes are of two types. 1) Sensor node which senses the data and routes it to sink node and 2) Sink node which collects data from sensor nodes. In case of hierarchical based network topology, the nodes are of three types: 1) sensor node which senses the

data and routes it to cluster head; 2) Sink node which collects data from sensor nodes and 3) cluster heads, which collects data from sensor nodes in its region, aggregate data and forwards it to sink node. Based on their functionality, the trust of each node can be calculated. As a result, the functionality trust is a trust factor which contributes to trust of a sensor node. The parameters of functionality are derived from other observed parameters such as communication parameters and data parameters, etc. As a result, in **Figure 1**, the functionality is shown with separate block, where it is derived from the observed information stored in Information storage. The functionality trust is evaluated based on observed functional parameters as follows:

***Functionality Trust* (*Sensor Node, Cluster Head, Sink*);**

If a node is not able to perform its functions in the network properly, those nodes a can be eliminated fro network based on functionality trust.

- Location Trust: The node trust has to be evaluated based on location information, if the routing algorithm is based on geographical location. The location trust is one of the factors for evaluation of trust of a neighbor node. Based on the current location information obtained, the node has to calculate its trust. The location trust is calculated based on parameters of LocX, LocY and Angle observed or explicitly obtained by the neighbor node as follows:

***Location Trust* (*LocX, LocY, Angle*);**

If the location informed by node *j* is same as location information calculated at node i, then node can be considered as trustworthy.

- Energy: Energy is one of the major factors in trust calculation. A neighbor node may have enough energy and may not cooperate for network functions which clearly indicates the node is a malicious node. A node may not be functioning properly as it is not having sufficient energy for communication. Care must be taken for not to take actions of the malicious node detection, in case of node is dead in the network.

***Energy Trust* (*Current Energy*);**

- Trust Update Time: This trust factor affects overall performance of a trust management system. If *trust update time* is less, most of the time a node may be busy in trust management rather than packet transfer. If the *trust update time* is large then the malicious nodes may get advantage of this and its activity may down the entire network. We consider that instead of having static *trust update time*, dynamically changing trust update time is better. The interval of trust update time can be considered based on the rate at which the events are occurring in the network.

***Trust Update Time* (*Event occurrence Time*);**

- Risk: Risk is the factor which is related to every other trust factor. If a certain amount of information is not available about the neighbor, then the factor of *Risk* has to be considered for evaluation of trust factors. The input for *Risk* function contain all other six trust factors as follows:

***Risk* (*Communication Trust, Data Trust, Functionality Trust, Location Trust, Energy Trust, Trut Update-Time*).**

3.3. Trust Model

Trust models are used to evaluate trust factors based on various theoretical concepts. The most widely used trust models are weighted mean, Bayesian model, subjective logic, entropy based model, fuzzy logic based model, game theoretic based model, human trust model, bio inspired models etc. The trust model mainly contains two major functions. 1) Calculate trust: The trust value is calculated based on trust factors and trust model 2) Update trust: the trust value is updated in the information storage.

We have considered only one type of trust model in this paper where other models can also be applied to the proposed trust management systems. The trust is defined as a belief level that one node can put on another node for specific action according to previous direct or indirect information of observations on behaviors. The belief level is the extent that one node believes that another node is willing to and able to obey the protocol and act normally. Let us consider an example, as a Bayesian based trust model. It is assumed that the subject node believes the object node behaves normally with probability θ, which can also be described as p(Belief). Here *Belief* denotes the trust in a node to perform normal behavior. Also, we use *Observation* to represent the observations one node obtains on another node. Then similar to [4], the formula for the standard Bayesian approach to be used for trust management can be provided as follows:

$$p(\text{Belief}/\text{Observation}) = \left[p(\text{Observation}/\text{Belief}) \cdot p(\text{Belief}) \right] / \text{Normalizing constant} \quad (1)$$

where *p*(Belief) is the prior probability, *p*(observation/Belief) is the posterior probability, *p*(Observation/Belief) is the likelihood function, and *p*(Belief/Observation) is the posterior probability.

Based on Ganeriwal *et al.*, [4] 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 $\alpha/(\alpha + \beta)$ according to Baye's and $(\alpha + 1)/(\alpha + \beta + 2)$ 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 neighboring node's behavior and build a trust for that node based on the observed information. The neighboring node's transactions are direct observations referred as first-hand information. For each observation, the node *i* maintains two parameters α and β which indicates the number of "successful" and "unsuccessful" operation by a neighbor node *j*.

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

The communication trust denoted as T_{ij}, is initialized to 0.5 based on Laplace Law. The Trust is calculated as shown in Equation (2) where α and β represents the number of "successful" and "unsuccessful" cooperation by node *j* to node *i* respectively.

As the sensor nodes are resource constraint, maintaining the history of all observed trials is resource consuming. To solve this issue, the α and β are updated periodically, based on *r* and *s* where *s* indicates number of "successes" and *r* indicates number of "unsuccessful" cooperation in a time window *t*.

$$\alpha_j = \alpha_j + r \quad \text{and} \quad \beta_j = \beta_j + r \tag{3}$$

Then α_j and β_j can be updated as shown in Equation (3).

$$\alpha_j = W_{age} \cdot \alpha_j + r \quad \text{and} \quad \beta_j = W_{age} \cdot \beta_j + r \quad \text{where} \quad 0 <= W_{age} <= 1. \tag{4}$$

As the data becomes old, the oldest information has to be discarded to provide a higher preference for latest information. Ganeriwal *et al.* [4] provides 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, we have proposed exponential decrease Bayesian Trust model to detect ONOFF attack in [9].

3.4. Applications for Trust Management in Wireless Sensor Networks

The trust management system can be used for various applications in wireless sensor networks. The application of trust management related to each layer of the protocol stack is shown in **Figure 1**.

- Application Layer: The data aggregation and cluster head selection are two major applications of the trust management system in the application layer. In case of hierarchical networks, the cluster head collects the sensor data from all sensor nodes, which are joined to the particular cluster head. The secure data aggregation needs to check a data stealthy attack, and aggregate data of only trusted nodes. Many of the hierarchical protocols for WSN selects a new set of cluster head in each round. The trust management system helps to identify trusted nodes for cluster head selection, thereby increases the security of the network.
- Transport Layer: Even though for simple sensed static data based wireless sensor network, UDP is sufficient. In case of multimedia wireless sensor networks, it needs TCP for streaming. As a result, it needs trust for end-to-end communication and trusted session operations which can be provided by the trust management system.
- Network layer: Each node in the network, sends or forwards the packet to sink node. The trust management in network layer basically has two roles. 1) Trusted neighbor identification: To identify a trusted neighbor for one hop communication; 2) Trusted routing path selection: The routing path must contain trusted path for communication in the network. Trust management can help to identify trusted nodes and trusted routing path in the network.
- Data link layer: The sensor node may try to access the network continuously in case of guaranteed services in MAC protocol of network. The DoS attack and unfairness access to channel can be dealt with trust management systems.

- Physical layer: The nodes in physical layer are prone to various kinds of attacks. The intrustion detection and reliable packet transfer at physical layer are main applications which needs trust management systems.

The complexity of the proposed framework, lies in observing neighbors based on specified parameters. As the nodes are resource constraint, watchdog techniques are costlier in terms of energy dissipation. The trust factors an be calculated based on observed trust parameters. Since, we assume nodes in network are static, it's enough to calculate trust based on direct observation. To converge the trust values faster, or if nodes are mobile, then it needs to consider indirect trust or recommendation trust, which further increases communication cost, as nodes should share their recommendations among its neighbours.

4. Simulation Results Discussion

The proposed trust management system is implemented in MATLAB for data aggregation and trusted routing applications along with intrusion detection. We have used the first order radio model for energy calculation. The sensor nodes are assumed to be deployed in an open environment. We use a tree based topology for routing in sensor network. The sink initiates process of routing. Every node observes each interaction with its neighbors and calculates trust during certain intervals of time. The malicious nodes are eliminated for further interactions in the network. The simulation details are explained in detail in following subsections.

4.1. Topology Creation

The sink node sends a beacon node which can reach up to radius R, where R is the communication range of a sensor node. When a sensor node, receives a beacon node, it initiates neighbor discovery based on HELLO packets and updates it's neighbor information table. We consider all nodes which are at one hop distance to sink node are first level parent nodes or cluster heads. A node sends a JOINREQUEST packet for requesting for join operations. The parent replies with JOINREPLY along with TDMA schedule or CDMA code for further communication. Once the first level parent node joins to Sink node, then it broadcasts the information along with number hops to sink as one of the parameters. When a node receives these broadcast packets, then based on the nearest distance from sink node, a second level node joins to its parent and further continues the process of sending broadcast messages. This process continues until all nodes in the network joins to the network. **Figure 2** shows the topology created for 100 nodes deployed in the area of 100 × 100 m area. The sink node is located at the center, and JOIN operation of each node is shown with dotted lines between two nodes. The node towards sink node are parent nodes for children nodes in the network.

4.2. Data Aggregation and Data Transfer

After a node joins to its parent node towards the sink, the node starts sensing the channel and sending data. The one level immediate parent node aggregates the data from its child and sends it to sink node. Each node checks for a stealthy attack before aggregating the data. We use standard deviation and Bayesian based estimation for trust calculation. If a node's data are within the range of valid data range calculated by standard deviation, then the operation is considered as "successful" operation else it is considered as "unsuccessful" operation. By taking it as α and β respectively, the trust model explained in Section 3.3 is used for calculating a node's trust with respect to data aggregation.

4.3. Attacker Model

Simulation is conducted for three kinds of attacks related to communication: Blackhole attack, Selective forward attack, and ONOFF attack, and one type of attacks related to data: Stealthy attack. In case of blackhole attack, a node drops all packets received from its neighbor. A selective forward attack, forwards the received packet to sink with a probability p. The ONOFF attack is one where a node initially forwards all the packets until it obtains a high trust value among neighbors. Later, periodically it forwards data (attacker is OFF) and drops the packets (attacker is ON). Data stealthy attack is a kind of attack where a node sends either very low or very high value to the cluster head instead of actually sensed value. This kind of attacks effects data aggregation value at cluster head.

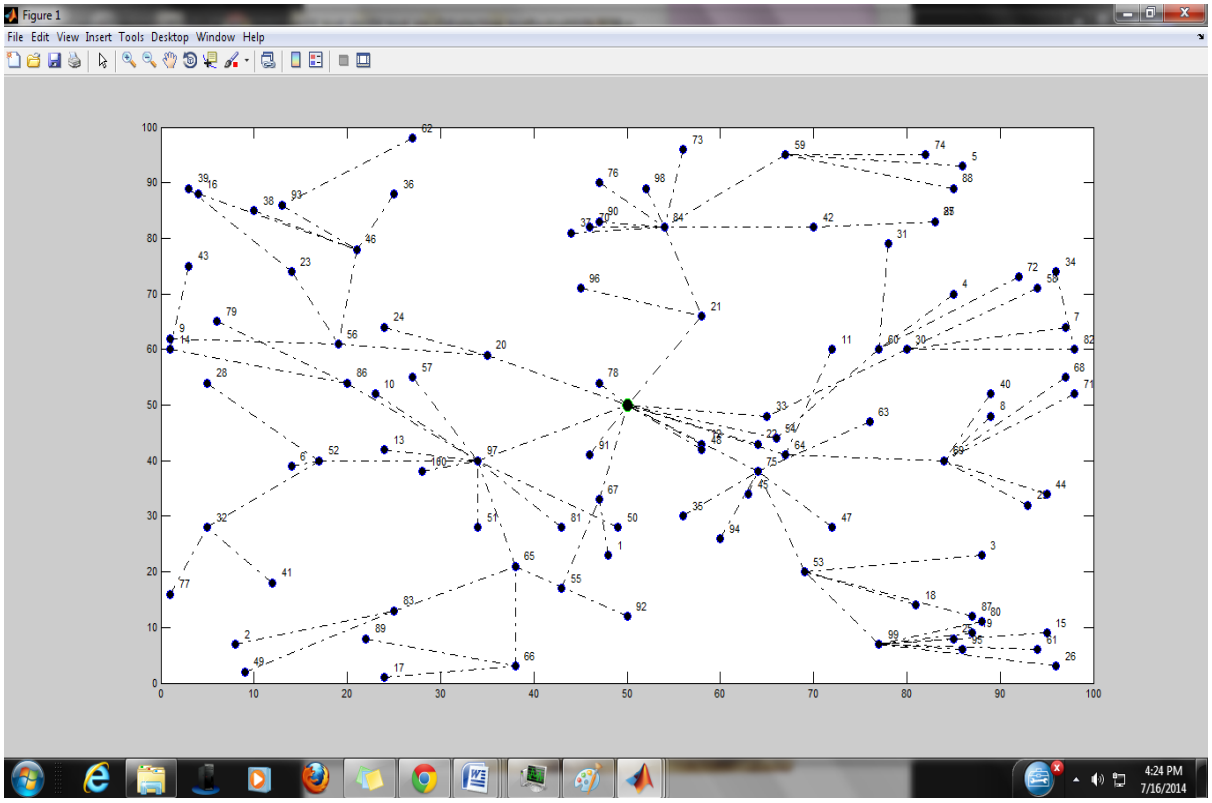

Figure 2. Topology of wireless sensor network for simulation.

4.4. Results and Discussions

The simulation is carried out for trust based secure communication and data aggregation along with intrusion detection for black holes, selective forward, ONOFF and stealthy attacks. The results are analyzed for 10%, 20% and 30% attacker nodes. The metrics used for comparison of results is based on True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The results are compared to standard Bayesian trust model (STM) with exponential decrease Bayesian trust model (ETM).

Table 1 shows the results for Black hole attack. In case of black hole attack, since all the packets are dropped by an attacker, the standard Bayesian trust model and proposed Exponential decrease Bayesian Trust model are able to identify the black hole attack 100% for scenarios with 10%, 20% and 30% attackers.

Table 2 shows the results for selective forward attack. The experiment is conducted for selective forward attack, where a node forwards the packet with a probability of 0.6. The results show that the exponential decrease Bayesian trust model is having 100% attacker detection compared to the standard Bayesian trust model.

Table 3 shows the results for ONOFF attack. ONOFF attack is an attack, where a node initially tries to establish high trust value in its neighbors and then starts dropping packet (ON) and forwarding packet (OFF) for a certain period of a time in the fashion of cycles. We can observe that, the standard Bayesian trust model, does not detect ONOFF attack, where the exponential decrease Bayesian model detects ONOFF attack with 100%. **Figure 3** shows percentage of True Positive (TP) for various kinds of attacks, with Standard and Exponential decrease Bayesian trust models. The results show that Exponential decrease trust model, performs better than Standard Trust model.

Table 4 shows the results of simulation with data stealthy attack. A stealth attack is one where a node simply sends either low or very high value as sensed data. This results in variation of aggregation value. The results are analyzed for 10%, 20% and 30% data stealthy attackers. The sensed value for the data stealthy attacker is analyzed for two different ranges. (i) Data with range (45 - 75) and (45 - 95). We can observe that the TP decreases as the number of attackers increases. As the number of nodes become stealthy attackers, the detection level decreases.

Table 1. Results of simulation with black hole attack.

Trust model	10% attacker nodes				20% attacker nodes				30% attacker nodes			
	TP	TN	FP	FN	TP	TN	FP	FN	TP	TN	FP	FN
Number of nodes in case of Standard Bayesian Trust Model	10	90	0	0	20	80	0	0	30	70	0	0
Number of nodes in case of Exponential Decrease Bayesian Trust Model	10	90	0	0	20	80	0	0	30	70	0	0

Table 2. Results of simulation with selective forward attack.

Trust model	10% attacker nodes				20% attacker nodes				30% attacker nodes			
	TP	TN	FP	FN	TP	TN	FP	FN	TP	TN	FP	FN
Number of nodes in case of Standard Bayesian Trust Model	9	90	0	1	18	80	0	2	27	70	0	3
Number of nodes in case of Exponential Decrease Bayesian Trust Model	10	90	0	0	20	80	0	0	30	70	0	0

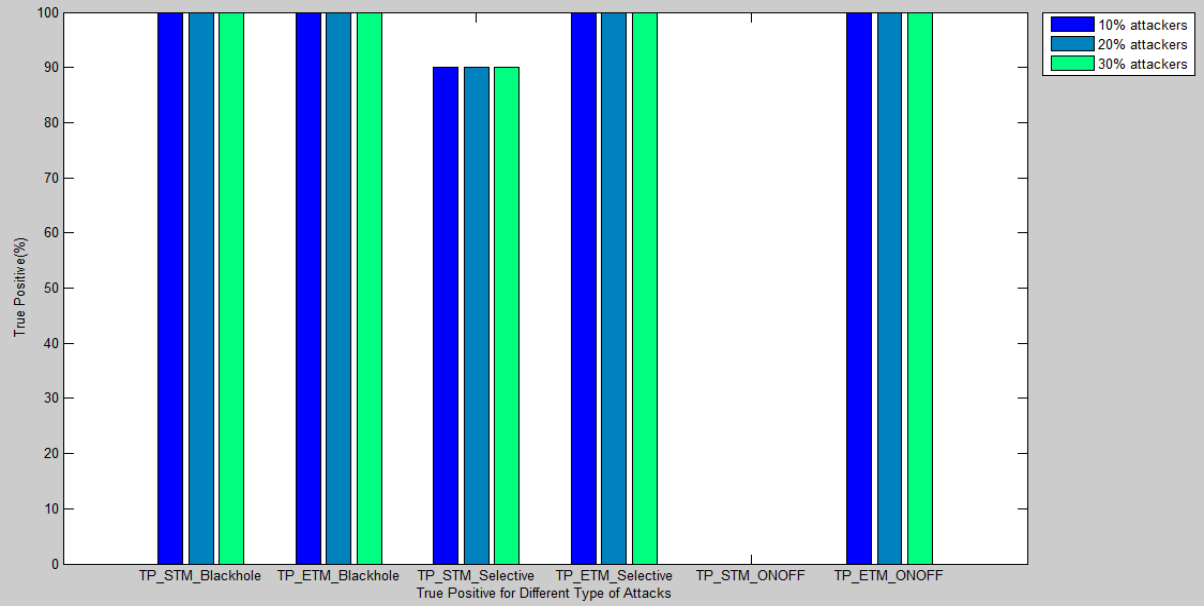

Figure 3. Analysis of True positive percentage for standard Bayesian trust model and Exponential decrease based trust model for various types of attacks.

Table 3. Results of simulation with ONOFF attack.

Trust model	10% attacker nodes				20% attacker nodes				30% attacker nodes			
	TP	TN	FP	FN	TP	TN	FP	FN	TP	TN	FP	FN
Number of nodes in case of Standard Bayesian Trust Model	0	90	0	10	0	80	0	20	0	70	0	30
Number of nodes in case of Exponential Decrease Bayesian Trust Model	10	90	0	0	20	80	0	0	30	70	0	0

The trust value of a benevolent node and a stealthy attacker is shown in **Figure 4** with respect data aggregation rounds. The result is taken for making a node as stealthy attacker after 20th round. The curve shows that the trust model decreases the thrust of the attacker, for each observation of stealthy attack hosted by a malicious node.

Trust management system, detects communication attacks such as blackhole attack (100%), selective forward attack (100%), ONOFF attack (100%). Data stealthy attack gets detected 100% if the number of attackers in the network are small. As the number of attacker nodes increases, the detection rate decreases (0%). It needs more sophisticated and robust technique for identifying data stealthy attacks. Our simulation has focused on attacker detection based on trust management system. Theoretically, detection of attacker and eliminating those nodes for further activities in the network, improves the performance, as the packets get transferred to sink node

Table 4. Results of simulation with stealthy attack.

Trust Model	10% attacker nodes				20% attacker nodes				30% attacker nodes			
	TP	TN	FP	FN	TP	TN	FP	FN	TP	TN	FP	FN
Number of nodes in case of Standard Bayesian Trust Model (data range 45 - 95)	10	90	0	0	19	80	0	1	15	70	0	15
Number of nodes in case of Standard Bayesian Trust Model (data range 75 - 95)	10	90	0	0	20	80	0	0	0	70	0	30
Number of nodes in case of Standard Bayesian Trust Model (data range 45 - 95)	10	90	0	0	20	80	0	0	30	70	0	0
Number of nodes in case of Standard Bayesian Trust Model (data range 75 - 95)	10	90	0	0	20	80	0	0	0	70	0	30

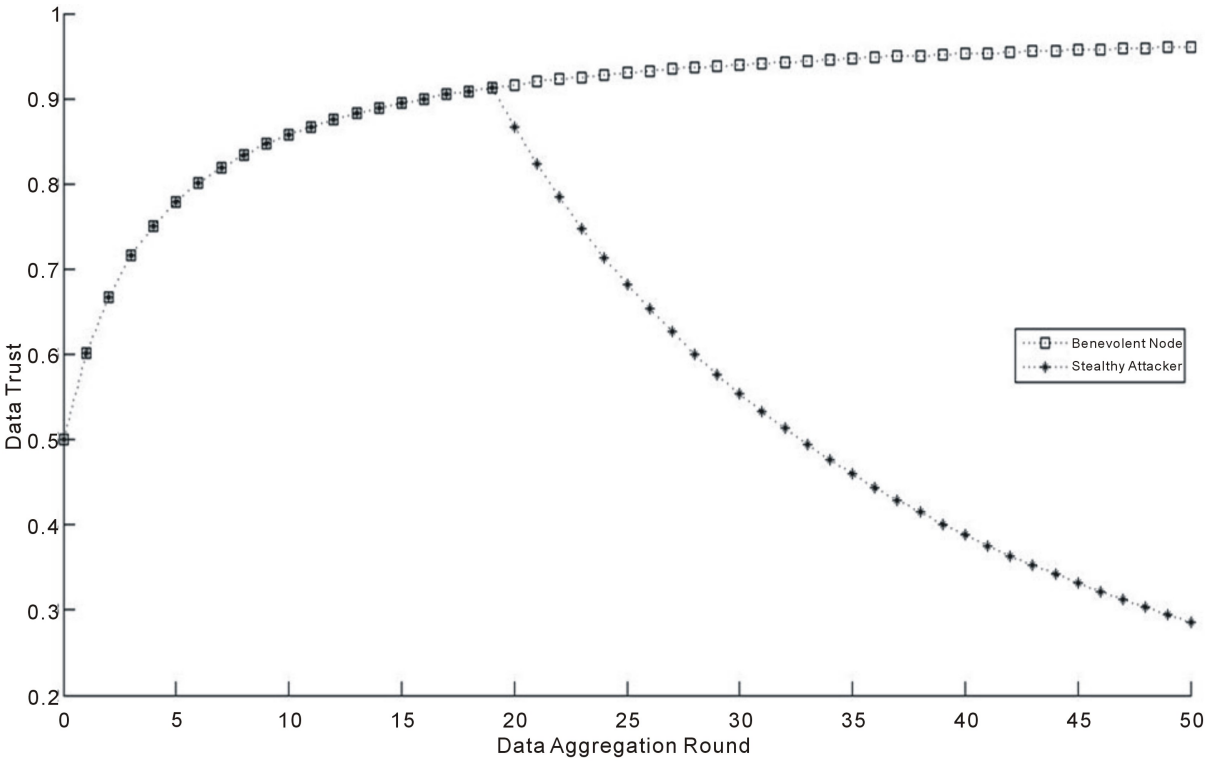

Figure 4. The trust value changes in benevolent and stealthy attacker for data aggregation rounds.

through trusted nodes in the network.

In summary, we have proposed a trust management system. The idea of simulation experiment is to show that the trust proposed trust management system can be used for various applications such as secure communication data aggregation, intrusion detection, etc. Even though we have analyzed very few applications here, we ensure that the trust management system along with proposed framework can be extended fro any kind of applications for secure communication in wireless sensor networks.

5. Conclusion

Wireless sensor network is an emerging technology for monitoring environment. The resource constraint sensor nodes are more vulnerable to attacks in wireless sensor networks as the nodes are deployed in open environment. A trust management system is essential for WSN, where cryptography techniques fail to address some issues. The frame work for secure communication and trust management systems are proposed in this paper. The simulation results show that the proposed model works for secure communication, data aggregation and intrusion. However, the proposed trust management system can be further extended for various other applications. This is an ongoing work, and as a future work we would like extend this work with more sophisticated trust models for various applications.

References

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) Wireless Sensor Networks: A Survey. *Computer Networks*, **38**, 393-422.

[2] Ishmanov, F., Malik, A.S., Kim, S.W. and Begalov, B. (2013) Trust Management System in Wireless Sensor Networks: Design Considerations and Research Challenges. *Transactions on Emerging Telecommunications Technologies*.

[3] Bao, F.Y., Chen, I.-R., Chang, M.J. and Cho, J.-H. (2012) Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrustion Detection. *IEEE Transactions on Network and Service Management*, **9**, 169-183.

[4] Ganeriwal, S., Balzano, L.K. and Srivastava, M.B. (2008) Reputation-Based Framework for High Integrity Sensor Networks. *ACM Transactions on Sensor Networks*, **4**, 1-37.

[5] Yao, Z., Kim, D. and Doh, Y. (2006) PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security. 2006 *IEEE International Conference on Mobile Adhoc and Sensor Systems* (*MASS*), Vancouver, October 2006, 437-446.

[6] Duan, J.Q., Yang, D., Zhu, H.Q., Zhang, S.D. and Zhao, J. (2014) TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, Article ID: 209436. http://dx.doi.org/10.1155/2014/209436

[7] Lopez, J., Roman, R., Agudo, I. and Fernandez-Gago, C. (2010) Trust Management Systems for Wireless Sensor Networks: Best Practices. *Computer Communications*, **33**, 1086-1093.

[8] Chen, H.G., Wu, H.F., Hu, J.C. and Gao. C.S. (2008) Event-Based Trust Framework Model in Wireless Sensor Networks. *Proceedings of International Conference on Neworking, Architecture, and Storage*, 359-364.

[9] 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*), **13**, 14-19.