A Trust-Based Scheme for Increasing Security in Wireless Sensor Networks

Mahdi Dibaei[1], Ali Ghaffari[2]
1, 2- Department of Computer Engineering, Tabriz branch, Islamic Azad University, Tabriz, Iran.
Email: Dibaeimahdi@yahoo.com
Email: A.Ghaffari@iaut.ac.ir

Received: June 2017 Revised: July 2017 Accepted: October 2017

ABSTRACT:
Security is considered to be one of the most important challenges in wireless sensor networks (WSNs). Due to inherent resource constraints in WSNs, traditional security mechanisms may not be used in these networks. In recent years, trust and reputation management in distributed systems has been proposed as a novel and accurate way for handling security deficiencies. Such deficiencies are deemed to be inherent in WSNs. Detecting malicious nodes is an important role of Trust models in WSNs. In line with reducing the above-mentioned deficiencies, this paper proposes a trust-based scheme for increasing security (TSIS) model for WSNs. The proposed trust-based scheme divides the network to several clusters. Inside each cluster, a special node named supervisor node is responsible for calculating the trusted values of other nodes. When supervisor nodes calculate trust value of other nodes within a cluster, they do not distribute these values. The receiver node requests the sender node authentication from its own supervisor node. The proposed method was simulated in the NS-2 environment. The simulation results indicate that the proposed method has improved energy efficiency and packet delivery rate. Hence, it has better performance than the earlier works with respect to the above-mentioned parameters.

KEYWORDS: Trust evaluation, Direct trust, Indirect trust, Supervisor node, Security, Wireless sensor networks.

1. INTRODUCTION

Recent advances in wireless communications and electronics have enabled the development of low-cost multifunctional sensors that exploit a physical phenomenon to provide data about the state of the environment. These tiny sensors have instigated the concept of Wireless Sensor Networks (WSNs) [1]. WSNs have been proven as a useful technology for perceiving information about the physical world. As a result, they have been used in many applications such as measurement of temperature, radiation, environmental monitoring, military surveillance, health care, disaster management, flow of liquids [2], [3], [36]. Microcontroller, transceiver circuits, memory, power source and sensor are main parts of a sensor node [4]. With the increased application of WSNs in military, commercial, and home environments; securing the data in the network has become a critical issue [5], [29-34].

Aside from the well-known vulnerabilities due to wireless communication, WSNs lack physical protection and are usually deployed in open, unattended environments which make them more vulnerable to attacks. Hence, it is crucial to propose plans with respect to the security of WSNs [6].

Nodes in a WSN have numerous constraints such as storage, communication, computational and processing capabilities, energy, etc. Considering these constraints is important in the development of security mechanisms for WSNs [7], [35-37].

In case a security measure is implemented for each attack, the security overhead will be overwhelmingly high for the (already scarce) available resources of the sensor network. In short, the desire to create a secure sensor network appears to be a challenging task. However, lately, sensor networks have found their way into real commercial applications. This offers the opportunity to use concrete practical scenarios and avoid making assumptions about abstract deployments [8].

The concept of trust in WSNs has been increasingly investigated by researchers and it is deemed to be an open question and a challenging issue. Although traditional mechanisms such as cryptography and intrusion detection systems can be possibly used against attacks, trust management systems which consume low energy are regarded as a more appropriate alternative for enhancing the security of these networks [9].

All kinds of transactions, interactions and communications in human life is based on trust. People always think about trust when they handle affairs, sometimes, unconsciously. So do the sensor networks. In sensor networks, one single node cannot do anything. Instead, they must co-work to accomplish higher level tasks. Therefore, they also need trust [10].

In this paper, trust-based scheme was used to enhance the security of WSNs. TSIS is proposed as a modified version of trust and centrality degree based access control model in wireless sensor networks (TC-BAC) [11] which uses trust but it is more energy-efficient than TC-BAC. Moreover, the rate of packet loss in the proposed method is less than those of other methods.

The rest of the paper is organized as follows: section 2 reviews some related works. Section 3 proposes trust modeling and the mechanism used for evaluating TSIS. Section 4 provides simulation-based analysis and evaluation of TSIS. Section 5 concludes this paper and suggests some future directions.

2. RELATED WORK

WSNs are vulnerable to several security threats but, due to limitations of WSNs in communication and processing, traditional security mechanisms such as cryptography cannot be applied in WSNs [12,13].

‘Trust’ is among highly complicated and puzzling concepts in social relationships. It is also a mental and psychological cognitive process which involves assumptions, expectations, behaviors, environments, and other factors [14].

The issue of trust management systems for WSNs is becoming of interest within the research community in the recent years, although it is still in an early state. Lots of efforts have gone in to the area of trust management systems for P2P or ad hoc networks. However, these systems do not fit all the requirements and features required by WSN. As mentioned, this research area has become very active and several surveys have been produced. Still, many of the solutions are designed with the purpose of solving very specific problems and most of them do not deal with all the features that a trust management system for WSN should provide [2].

In the following, we will provide an overview of the state of the art in trust management for WSN. Generally speaking, node trust models can be classified in to two categories: centralized and distributed models. In centralized trust models, a particular trusted intermediary or base station is used to calculate trust values of sensor nodes. In distributed trust models, sensor nodes calculate trust values by themselves [15].

A distributed reputation-based framework for sensor networks (RFSN) is proposed in [16] which calculates reputation scores based on similarity of data reported by sensors with overlapping coverage. RFSN uses density based outlier detection to generate reputation scores, integrates reputation scores into a trust score using a Bayesian formulation and lowers trust scores over time if they are not refreshed. Privilege of this investigation is the experimental design: the authors simulate their design, implement it and collect data in both lab and operational environments system model [17].

In 2008 Kim and Seo proposed a central trust model using fuzzy logic in wireless sensor network [18]. This method formulates the trust model using fuzzy logic for the safe communication to choose suitable paths between source and destination node in wireless sensor network. To calculate the trust level of sensor node, it defines T as trustworthiness and U as untrustworthiness. The range of T and U are $0\leq T\leq 1$ and $0\leq U\leq 1$. It assumes that base station in wireless sensor network has the reputation value of each sensor node. Then it calculates evaluation value for paths from source to destination and uses the path that has high trust value to transmit packets safely to the destination sensor node without considering the attack of abnormal sensor.

A distributed trust computation scheme, named parameterized and localized trust management scheme (PLUS) is proposed in [10]. In this scheme each sensor nodes rates the trustworthiness of its interested neighbors and share its opinion about neighbor nodes. To use nodes opinion about their neighbors, it defines three roles to nodes: the node, which performs evaluation, as judge; the node, which is in the radio range of the judge and will be evaluated, as suspect; and the node, which maintains the trust value of the same suspect with the judge and sends out the corresponding opinion periodically or intentionally as jury. When a node communicates with other node has one of these three roles.

Shaikh et al. [19] have proposed a group-based trust management scheme (GTMS) for clustered wireless sensor networks. GTMS divides Trust calculation to three phases: trust calculation at node level, trust calculation at Cluster Head level and trust calculation at Base station level. At node level it calculates trust value with an equation that relates successful and unsuccessful interactions in different timing windows, Δt. GTMS assumes that the cluster heads have higher memory and computational power than other nodes. In many cluster based methods like low-energy adaptive clustering hierarchy (LEACH) [20] cluster heads differ from one round to another and it may not possible to assign higher memory and computational power to CH nodes. GTMS also do not consider current behavior of a node in trust evaluation and only rely on the history of past transactions.

Collaborative lightweight trust management scheme (CLT) [21] derives the trust, based on direct trust and indirect trust. It also uses time window mechanism to store history of trust values and equations that relate successful and unsuccessful transactions for calculating trust value similar to what it is used in GTMS [19]. CLT uses IEEE 802.15.4 MAC protocol. Rather than indirect trust overhead, for evaluating direct trust, TCL sends acknowledgment packets to subject node from a different path and this increase the overhead of this method. TCL uses indirect trust when there is not direct trust relationship between subject and target nodes.

TC-BAC [11] is a trust and centrality degree based access control model in wireless sensor networks proposed in 2013. Both of direct trust and indirect trust are used in this model. This method discusses trust evaluation in single domain and multi domain in wireless sensor networks. The most important defect of TC-BAC is that indirect trust in trust evaluation of nodes causes high energy consumption.

3. THE PROPOSED TRUST-BASED SECURITY MODEL

3.1. Architecture of Trust Management

In this section, a novel trust-management model named TSIS is proposed. In this paper, it was assumed that WSN nodes are divided into some clusters. A node called supervisor node was placed in every cluster to supervise data flows of cluster nodes and calculate a trust value for each node within a cluster. The most important purpose of TSIS model is to protect information and network operations against malicious nodes. The malicious nodes can be considered as agents which are out of a network or the infected nodes inside the network which have been attacked and compromised by other malicious agents. Malicious nodes try to introduce themselves as a network node and after joining the network, they start to attack other nodes in the network.

Fig. 1 depicts the architecture of the proposed model. Using some detecting mechanisms, network nodes can detect the behaviors of malicious nodes such as worm holes [22, 23], sink holes [24], etc. In the TSIS model, the trust of an arbitrary node is composed of two major parts: direct trust and supervisor trust. The first one is based on direct conception and impression of a node about the behaviors of its neighbors when it communicates with them. The latter part of a trust is based on the trust which has been calculated by the supervisor node of the cluster. The supervisor node supervises the data flow between the nodes of a cluster. The history of nodes' direct trusts about their neighbors is stored in history data storage unit.

As shown in Fig. 2, in the proposed TSIS model, each cluster has a supervisor node which is responsible for supplying security in its cluster. Each supervisor node has a trust table inside its memory and produces a trust value for every node of the cluster. Each supervising node supervises the data flow inside the clusters and uses some detection mechanisms to detect malicious nodes. In multi-domain WSNs, there is a trust center which is composed of one or more supervisor nodes which are responsible for evaluating inter-domain trust. In the TSIS model, trust evaluation equations are presented in the next two sections. First, trust evaluation equations in single-domain WSNs are presented; then, multi-domain WSN equations are presented which have been derived from single-domain WSNs.

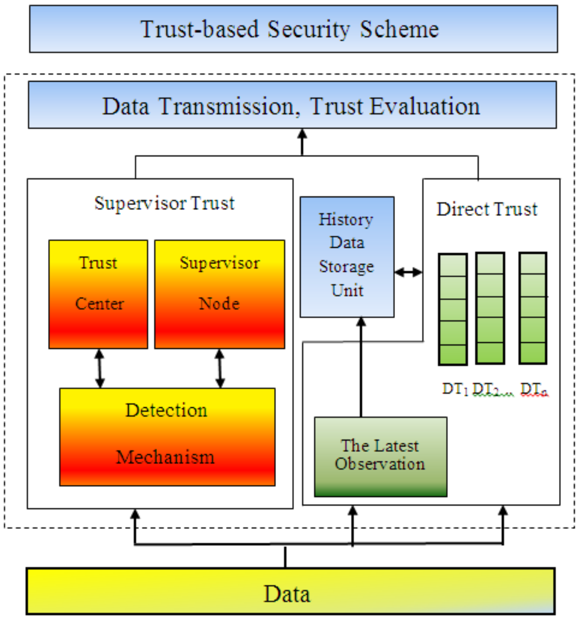

Fig.1. Architecture of TSIS model. Trust of an arbitrary node is composed of two major parts: direct trust and supervisor trust.

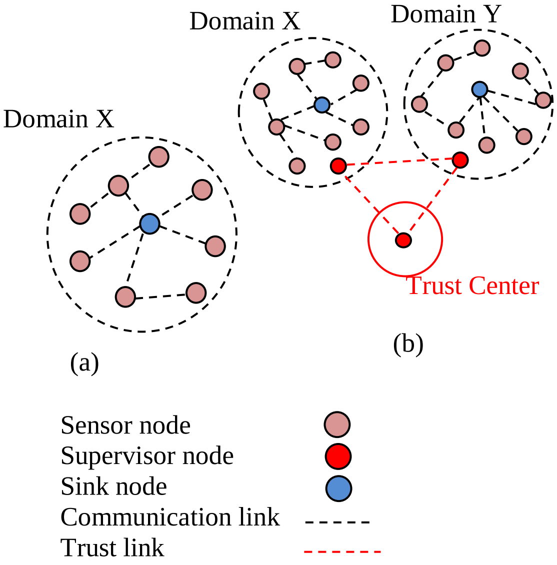

Fig.2. (a) TSIS model in single-domain and Multi-domain (b). In multi-domain WSNs, there is a trust center.

3.2. Trust Evaluation in a Single-domain WSNs

This section presents the equations for evaluating trust values in single domain WSNs and the next section will extend these equations to evaluate trust values in multi-domain WSNs. In single-domain WSNs, the trust of node i to node j is calculated by the following equation:

$$T(i_x, j_x)^L = \alpha_1 DT(i_x, j_x)^L + \beta_1 ST(S_x, j_x)^L \qquad (1)$$

$\alpha_1 + \beta_1 = 1, \alpha_1 > 0, \beta_1 > 0.$

Where $DT(i_X,j_X)$ represents the direct trust of node i to node j in domain X. The index x in i_X and j_X shows that node i and node j are in domain X. $ST(S_X,j_X)$ refers to the supervisor node's trust to node j in domain X. In Eq. (1), L value indicates the sequence number of the latest evaluation records. The value α_1 and β_1 are weight factors. Setting $\alpha_1 > \beta_1$ indicates that direct trust of nodes is important than recommendations by supervisor nodes and Setting $\alpha_1 < \beta_1$ indicates that recommendations by supervisor node is important than direct trust.

Each node in a domain has a trust table that is composed of trust values of other nodes in the domain and when nodes communicate with their neighbors inside domain, they update these trust values. Direct trust (DT) of node i to node j in a single domain X which was used in Eq. (1) is calculated as follows:

$$DT(i_X, j_X)^L = \gamma DT(i_X, j_X)^{L-1} + E(i_X, j_X)^L \qquad (2)$$

Where:

$$E(i_X, j_X)^L = \begin{cases} P(a) & 0 < P(a) < 1 \\ N(a) & 1 < N(a) < 0 \end{cases} \qquad (3)$$

$\gamma > 0$. In Eq. (3), $P(a)$ and $N(a)$ represent positive and negative values, respectively. If the behavior of node j with node i in the current transaction is evaluated as a good behavior, then, node i will consider a positive number as a trust value to node j. Otherwise, if the behavior of node j in the current transaction is evaluated to be malicious towards node i, then, node i will consider a negative number as the trust value about node j. In Eq. (2), L value indicates that the trust values belong to the current transaction and $L-1$ indicates that the trust values belong to the last transactions or recommendations. In Eq. (1), the trust of supervisor node to node j in domain X is calculated as follows:

$$ST(S_X, j_X)^L = \gamma ST(S_X, j_X)^{L-1} + E(i_X, j_X)^L \qquad (4)$$

$\gamma > 0$. In Eq. (3) and Eq. (4), γ is the weight factor that shows how much trust values that have been calculated at previous transactions are important.

3.3. Trust Evaluation in Multi-domain

When a WSN has more than one domain so that node i in domain X intends to calculate a trust value for node j in the domain Y, then, the trust evaluation between nodes will be more complicated. In these situations, since nodes i and j belong to different domains and do not have direct communication with each other, hence, the trust of domain X to domain Y should be considered. To do this, a trust center was defined in this paper which is depicted in Fig. 2 (b). Indeed; the trust center is composed of supervisor nodes which are responsible for evaluating inter-domain trust. Node i in domain X calculates a trust value about node j in domain Y via the following equation:

$$T(i_X, j_Y)^L = M(X, Y)^L \times ST(S_Y, j_Y)^L \qquad (5)$$

In Eq. (5), $ST(S_Y,j_Y)$ denotes the trust value which supervisor node calculates about node j in domain Y. The value of $M(X, Y)$ is calculated by the following equation:

$$M(X, Y)^L = \alpha_2 ST(S_X, S_Y)^L + \beta_2 TCT(S_{TC}, S_Y)^L (6)$$

$\alpha_2 + \beta_2 = 1, \alpha_2 > 0, \beta_2 > 0$

In Eq. (6), $ST(S_X, S_Y)$ refers to the trust value which the supervisor node in domain X calculates about the supervisor node in domain Y. The value of $TCT(S_{TC}, S_Y)$ denotes the trust value which the supervisor node in the truest center calculates about the supervisor node in domain Y.

When a sender node communicates with a receiver node, the sender node should evaluate a trust value about receiver node. Fig. 3 depicts this procedure. When node i in domain X wants to send data to node j in domain Y, before sending data, node i should evaluate a trust value about node j. So node i asks the supervisor node of domain X to do this with $T(i_X,j_Y)$. Then supervisor node of domain X asks the trust value of node j from supervisor node of domain Y with $ST(S_Y,j_Y)$. The supervisor node of domain Y replies the trust value of node j by $ST(S_Y,j_Y)$. Supervisor node of domain X has a trust value about supervisor node of domain Y which has been shown with $ST(S_X,S_Y)$ in Eq. (6). To enhance reliability, supervisor node of domain X also request a trust value about supervisor node of domain Y from trust center. So it requests from trust center by Req. $TCT(S_{TC},S_Y)$ and trust center reply with Rep. $TCT(S_{TC},S_Y)$. Now supervisor node of domain X calculates a trust value about node j in domain Y by Eq. (5).

The trust center is responsible to supervise the behavior of supervisor nodes of domains and calculates and keeps trust values about supervisor nodes of domains. Only supervisor nodes can communicate with Trust center with a cryptography method and other nodes cannot do this because of security issues. TSIS method calculates a trust value for a node which ranges from 0 to 100 through equations (1) to (6).

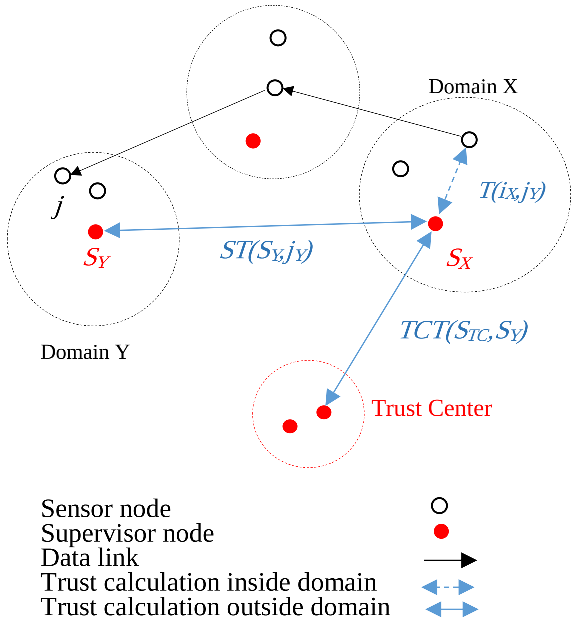

Fig.3. Trust evaluation in multi-domain WSNs and the role of trust center.

A mapping mechanism maps this value to a number from 0 to 7. This trust value is stored in three bits and uses less memory. Algorithm 1 is the pseudo code of TSIS model. First, sensor nodes are organized in some clusters. Then, a supervisor node for each cluster is determined. Then, the trust tables of the supervisor nodes are initialized with the value of 50. Then, as far as the nodes are alive and sense their environment, supervisor nodes will supervise data flow of the network and will serve as consultants for other nodes.

Algorithm 1: TSIS model algorithm

```
for i=1  to Sensornum
     Divide sensor nodes into some clusters
end for
for i=1  to Clusternum
     Choose a supervisor node in each cluster
     Initialize trust tables of supervisor nodes
     with the value of 50
end for
While Energy> 0
     Update trust tables when an event occurs
 end while
END
Notations:
          Sensornum: Number of all sensors
          Clusternum: Number of clusters
          Energy: Total energy of all nodes
```

4. PERFORMANCE EVALUATION OF TSIS

TSIS method was simulated and the results were analyzed and compared with other schemes. NS-2 [25] and MATLAB [26] were used to simulate the TSIS method. On average, the simulation was repeated 10 times and a mean value for the results was calculated. Simulation parameters have been summarized in table 1. In this paper, two major types of nodes were used: ordinary nodes and supervisor nodes. At the first step of simulation, all nodes were distributed in the area. Then, the nodes were divided into 4 clusters. Every supervisor node was allocated to a central area inside a cluster and other nodes within that cluster were able to communicate directly with the supervisor node. Therefore, in the proposed method, the following operations were executed: clustering, finding the supervisor node within each cluster, initializing trust tables, updating trust values. It should be noted that the operation of initializing trust values was conducted in the memory of the supervisor nodes with the value of 50. The values (50) will be updated according to the behavior of nodes.

Table 1. The simulation parameters.

Parameters	**values**
Simulation time	25 s
Monitoring area	800 × 800 m2
Number of nodes	20,100
Propagation model	Two ray
Number of malicious nodes	1
Type of attack	DOS attack
Packet interval	0.5 s
Length of data packet	1000 bytes
Initial energy	20 J
Transmit power	0.9 w
Receive power	0.8 w
Idle power	0.1 w
Sense power	0.0175 w
Routing protocol	AODV
MAC layer protocol	IEEE 802.11

4.1. Analyzing Energy Consumption in the Proposed TSIS Model

One of the most critical challenges in WSNs is the reduction of energy consumption [3]. Data communication consumes energy significantly more than data processing does. The energy consumption for transmitting 1KB of data in a distance of 100 m is almost equal to executing 3 million instructions with a 100 MIPS[1] processor [27]. In the proposed TSIS method, the trust value of each node was calculated by the supervisor node. Unlike the methods based on indirect trust, communicating with neighboring nodes of a target node is not necessary for evaluating trust; consequently, it can be argued that the TSIS method reduces the energy

[1] Millions Instructions Per Second

consumption.

Fig. 4 demonstrates energy consumption in a WSN in four different conditions. The characteristics of the used WSN are mentioned in table 1. A WSN without any attack has less energy consumption than other methods. A WSN affected by a DOS attack (denial of service) [28] with one malicious node has no security method and consumes more energy than other methods. As illustrated in Fig. 4, it can be observed that TC-BAC consumes more energy than TSIS method. In simulating both methods, a DOS attack with one malicious node was assumed.

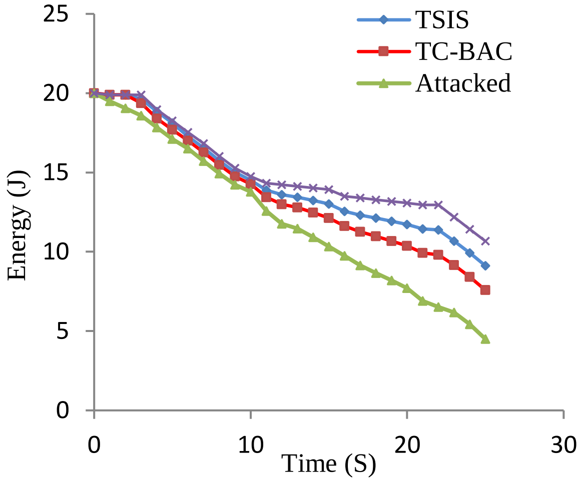

Fig.4. Energy consumption with 100 nodes.

In the next simulation, the size of WSN was changed including 20 nodes and the energy consumption for the four different scenarios was measured again. As depicted in Fig. 5, the general trend in energy consumption did not change in all the four scenarios. It can be noted from the following figure that the energy efficiency of TSIS is better than TC-BAC.

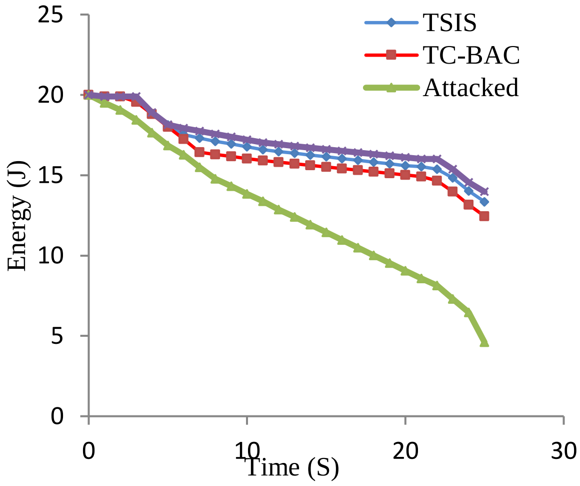

Fig.5. Energy consumption with 20 nodes.

4.2. Analyzing Packet loss

Packet loss is defined as the fraction of packets which are not received successfully within a certain time span. Packet loss is considered to be one of the major problems in WSNs. Fig. 6 compares Packet loss between TC-BAC and TSIS methods in a 20-node WSN. Results of this comparison reveal that packet loss in TC-BAC is more than that of TSIS. This adds to the merits of the TSIS model proposed in the present paper.

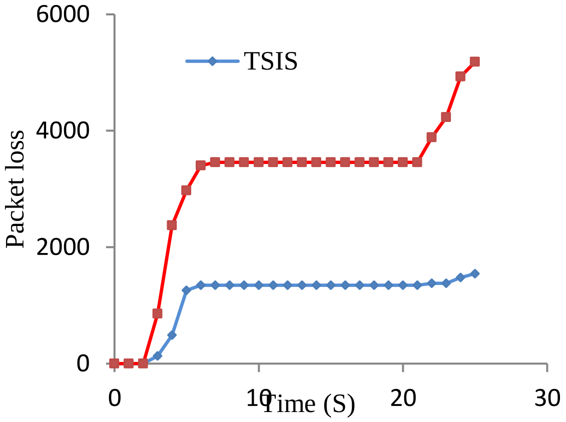

Fig.6. Packet loss with 20 nodes.

4.3. Analyzing Overhead

In this section, the proposed method was analyzed and evaluated in terms of overhead. To do this, the number of communications for trust evaluation in TSIS was compared with those of TC-BAC. 100 nodes were clustered in 4 equal clusters. Each cluster included a supervisor node. In next simulations, one parameter was manipulated and its effects on the number of communications were measured. As shown in Fig. 7, approximately 900 communications were required for 400 events in the TC-BAC method. However, in the TSIS method, 400 communications were required for 400 events. Hence, the overhead of the TSIS is lower than that of TC-BAC.

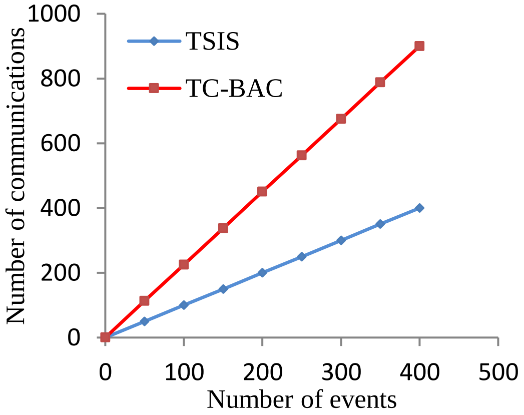

Fig.7. Number of communications including 100 nodes.

In Fig. 8, the number of nodes changed to 200. Other parameters were left unchanged. As shown in Fig. 8, the behavior of methods does not change. The energy consumption in TC-BAC with 200 nodes is the same as the energy consumption of TC-BAC with 100 nodes. However, that is not the case with the TSIS method. That is to say, in the TSIS method, almost 2000 communications are required for 400 events.

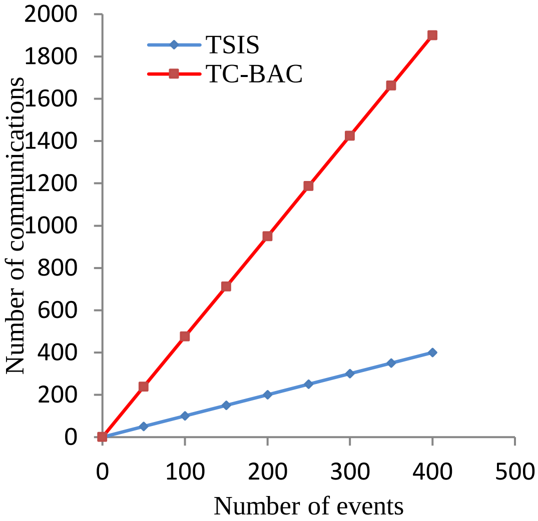

Fig.8. Number of communications with 200 nodes.

In Fig. 9, communication range of the nodes is 150m. The results indicate that the change of communication range affects the number of communications for trust evaluation in TC-BAC. In TSIS, with a communication range of 150 m, the number of required communications for evaluating the trust of 400 events is less than the number of required communications in the communication range of 100 m.

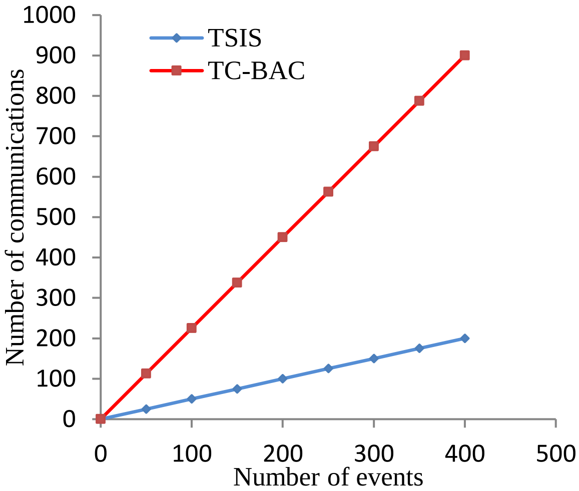

Fig.9. Number of required communications in 150m communication range.

Once a communication between two nodes is completed, in case node i wants to begin another communication with node j, it (node i) should calculate a trust value for node j. To do this in TC-BAC model, node i should ask the neighbors of node j about its trust (trust of node j) (indirect trust). If it is assumed that node j has 4 neighbors, node i should ask four nodes about the trust value of node j. In contrast, in TSIS model, since there is a supervisor node in each cluster, node i only asks the supervisor node about the trust value of node j. Thus, if every node has n neighbors, then, the overhead of TC-BAC and other models using the indirect trust will increase with factor n in each communication.

5. CONCLUSION

In this paper, a trust-based model for increasing security in clustered WSNs was presented. Supervisor nodes were introduced to detect malicious nodes in TSIS model. The results of the simulations revealed that the TSIS has significantly better performance than previous methods in terms of the following parameters: the number of required communications for trust evaluation, energy consumption of the nodes and packet loss.

REFERENCES

[1] S. V. Vajdi, A. R. Hilal, S. A. Abeer, and O. A. Basir, **"Multi-hop Interference-Aware Routing Protocol for Wireless Sensor Networks,"** *Procedia Computer Science*, Vol. 10, pp. 933-938, 2012.

[2] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, **"Trust management systems for wireless sensor networks: Best practices,"** *Computer Communications*, Vol. 33, pp. 1086-1093, 2010.

[3] M. Azharuddin, P. Kuila, and P. K. Jana, **"Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks,"** *Computers & Electrical Engineering*.

[4] I. Banerjee, P. Chanak, H. Rahaman, and T. Samanta, **"Effective fault detection and routing scheme for wireless sensor networks,"** *Computers & Electrical Engineering*, Vol. 40, pp. 291-306, 2014.

[5] J. Lee, K. Kapitanova, and S. H. Son, **"The price of security in wireless sensor networks,"** *Computer Networks*, Vol. 54, pp. 2967-2978, 2010.

[6] L. B. Oliveira, A. Ferreira, M. A. Vilaça, H. C. Wong, M. Bern, R. Dahab, *et al.*, **"SecLEACH—On the security of clustered sensor networks,"** *Signal Processing*, Vol. 87, pp. 2882-2895, 2007.

[7] J. Yick, B. Mukherjee, and D. Ghosal, **"Wireless sensor network survey,"** *Computer Networks*, Vol. 52, pp. 2292-2330, 2008.

[8] A. A. Cardenas, T. Roosta, and S. Sastry, **"Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems,"** *Ad Hoc Networks*, Vol. 7, pp. 1434-1447, 2009.

[9] Y. Yu, K. Li, W. Zhou, and P. Li, **"Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures,"** *Journal of Network and Computer Applications*, Vol. 35, pp. 867-880, 2012.

[10] Z. Yao, D. Kim, and Y. Doh, **"PLUS: Parameterized and localized trust management scheme for sensor networks security,"** in *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*, 2006, pp. 437-446.

[11] J. Duan, D. Gao, C. H. Foh, and H. Zhang, **"TC-BAC: A trust and centrality degree based access control model in wireless sensor networks,"** *Ad Hoc Networks,* Vol. 11, pp. 2675-2692, 2013.

[12] Ghaffari, A., Rahmani, A. M. (2008, August). **"Fault tolerant model for data dissemination in wireless sensor networks".** In *Information Technology, 2008. ITSim 2008. International Symposium on*, Vol. 4, pp. 1-8, IEEE.

[13] A. Boukerch, L. Xu, and K. El-Khatib, **"Trust-based security for wireless ad hoc and sensor networks,"** *Computer Communications,* Vol. 30, pp. 2413-2427, 2007.

[14] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, **"Trust prediction and trust-based source routing in mobile ad hoc networks,"** *Ad Hoc Networks,* Vol. 11, pp. 2096-2114, 2013.

[15] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, **"Management and applications of trust in Wireless Sensor Networks: A survey,"** *Journal of Computer and System Sciences,* Vol. 80, pp. 602-617, 2014.

[16] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, **"Reputation-based framework for high integrity sensor networks,"** *ACM Transactions on Sensor Networks (TOSN),* Vol. 4, p. 15, 2008.

[17] R. Mitchell and I.-R. Chen, **"A survey of intrusion detection in wireless network applications,"** *Computer Communications,* Vol. 42, pp. 1-23, 2014.

[18] T. K. Kim and H. S. Seo, **"A trust model using fuzzy logic in wireless sensor network,"** *World academy of science, engineering and technology,* Vol. 42, pp. 63-66, 2008.

[19] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, **"Group-based trust management scheme for clustered wireless sensor networks,"** *Parallel and Distributed Systems, IEEE Transactions on*, Vol. 20, pp. 1698-1712, 2009.

[20] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, **"Energy-efficient communication protocol for wireless microsensor networks,"** in *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, Vol. 2, pp. 10, 2000.

[21] X. Anita, M. Bhagyaveni, and J. M. L. Manickam, **"Collaborative Lightweight Trust Management Scheme for Wireless Sensor Networks,"** *Wireless Personal Communications,* pp. 1-24, 2014.

[22] Y.-C. Hu, A. Perrig, and D. B. Johnson, **"Packet leashes: a defense against wormhole attacks in wireless networks,"** in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies,* 2003, pp. 1976-1986.

[23] Y.-C. Hu, A. Perrig, and D. B. Jo**hnson, "Wormhole attacks in wireless networks,"** *Selected Areas in Communications, IEEE Journal on,* Vol. 24, pp. 370-380, 2006.

[24] E.-H. Ngai, J. Liu, and M. R. Lyu, **"On the intruder detection for sinkhole attack in wireless sensor networks,"** in *Communications, 2006. ICC'06. IEEE International Conference on*, 2006, pp. 3383-3389.

[25] K. Fall and K. Varadhan, **"The ns Manual (formerly ns Notes and Documentation),"** *The VINT project,* Vol. 47, 2005.

[26] M. U. s. Guide, **"The mathworks,"** *Inc., Natick, MA,* Vol. 5, 1998.

[27] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, **"Wireless sensor networks: a survey,"** *Computer Networks,* Vol. 38, pp. 393-422, 2002.

[28] A. Wood and J. A. Stankovic, **"Denial of service in sensor networks,"** *Computer,* Vol. 35, pp. 54-62, 2002.

[29] Ghaffari, Ali. **"Designing a wireless sensor network for ocean status notification system."** *Indian Journal of Science and Technology* 7, No. 6, pp. 809-814, 2014.

[30] Ghaffari, Ali. **"Congestion control mechanisms in wireless sensor networks: A survey."** *Journal of network and computer applications* 52, pp. 101-115, 2015.

[31] Ghaffari, Ali. **"Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms."** *Wireless Networks* 23, No. 3, pp. 703-714, 2017.

[32] Masoudi, Rahim, and Ali Ghaffari. **"Software defined networks: A survey."** *Journal of Network and Computer Applications* 67, pp. 1-25, 2016.

[33] Nikokheslat, HosseinDabbagh, and Ali Ghaffari. **"Protocol for Controlling Congestion in Wireless Sensor Networks."** *Wireless Personal Communications*: 1-19.

[34] Ghebleh, Reza, and Ali Ghaffari. **"A Multi-criteria Method for Resource Discovery in Distributed Systems Using Deductive Fuzzy System."** *International Journal of Fuzzy Systems*: 1-11.

[35] KeyKhosravi, Davood, Ali Ghaffari, Ali Hosseinalipour, and BatoolAbadiKhasragi. "**New Clustering Protocol to Decrease Probability Failure Nodes and Increasing the Lifetime in WSNs."** *Int. J. Adv. Comp. Techn.* 2, No. 2, pp. 117-121, 2010.

[36] Azari, Leila, and Ali Ghaffari. **"Proposing a novel method based on network-coding for optimizing error recovery in wireless sensor networks."** *Indian Journal of Science and Technology* 8, No. 9, pp. 859-867, 2015.

[37] Molani, M., Ghaffari, A., & Jafarian, A. **"A new approach to software project cost estimation using a hybrid model of radial basis function neural network and genetic algorithm"**. *Indian Journal of Science and Technology*, *7*(6), pp. 838-843, 2014.