I.J. Wireless and Microwave Technologies, **2017, 6, 58-67**
Published Online November 2017 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2017.06.06

Available online at ***http://www.mecs-press.net/ijwmt***

A Trust-based Security Approach in Hierarchical Wireless Sensor Networks

Mohsen Salehi[a], Jamal Karimian[b]

[a,b] *Department of Computer Engineering, Imam Reza International University, Mashhad, Iran*

Received: 10 March 2017; Accepted: 17 June 2017; Published: 08 November 2017

Abstract

In recent decades Significant expansion and popularity of wireless sensor networks in various applications have attracted the attention of many researchers. The main challenges of WSN for the researchers are Energy and security restrictions. Recently trust as a new, efficient and soft method has been able to provide satisfactory security in WSN. In this study by using a simple method, first each node calculates the trust values of neighbors and according to these values exchanges data with neighbor nodes, then from each cluster, a node whose trust is greater than a threshold value can be candidate for being cluster head. Finally by using fuzzy logic a node with the most trusted neighbors and desirable energy level among the candidate nodes is selected as a cluster head. Simulation results show that proposed system has been able to greatly improve security and prevent untrusted and malicious nodes from becoming the cluster head.

Index Terms: Wireless Sensor Network, Trust, Security, Cluster Head, Fuzzy Logic

1. Introduction

A wireless sensor network consists of a large number of sensor nodes that collect information from the environment. The high ability of these networks to communicate with natural phenomena led to the expansion of these networks in many applications such as military, commercial, intrusion detection, etc. [1]. The structure and architecture of these networks caused to several challenges, most notably are energy and security restrictions. Most of these networks due to their placement in open environments without protection are exposed to direct attacks.

Many recent studies such as authentication, key agreement and encryption have created a relative security for

* * Corresponding author. Tel.: +989124741556
E-mail address: Mohsen.salehi@Imamreza.ac.ir

WSNs and prevent the malicious nodes intrusion from outside to the internal network. In WSNs, malicious sensor node can be an outside malicious node, a trapped or controlled sensor node. Since outside malicious sensor nodes don't have the network key can't obtain authentication ID, so can't achieve the required primary trust. therefore, the traditional authentication system can easily identify these nodes, but for internal malicious sensor nodes, it's easy to launch attacks because these nodes have the network key which invalidates traditional authentication system. Hence, old security solutions based on encryption and authentication are not enough for wireless sensor networks which confront with new challenges of insider attacks. This necessitates a new, efficient and trust solution which known as a new way to deal with this type of attacks [2].

This paper focuses on providing an efficient and secure trust-based method for WSNs that reducing resource consumption, resistant against external and insider attacks. The Network considered in this paper is two-level clustering. One of the main objectives of this study is clustering head selection mechanism by using trust and fuzzy logic. In the second section of this paper, a brief description of the related work was provided. The third section discussed the proposed system and its component. Finally experimental results, conclusion and future work are expressed.

2. Related Work

In recent years, trust-based solutions have been widely used in wireless sensor networks. Research in this area can be considered in three type includes trust-based routing; secure data aggregation with the contribution of trust and trust-based solutions for the cluster head selection [3]. In the following, some studies in this area are briefly reviewed. Paper [4] consists of two main parts of monitoring and reputation system. The monitoring system task is to monitor the behaviour of neighbouring nodes and reputation system which responsible for maintaining the reputation of the node. In such system, the beta distribution was used to calculate the trust.

The authors of [5] used a combination of direct and indirect trust to calculate the trust of each node. Direct trust is calculated based on the usability of each node and the number of correct packets exchanged, and indirect trust is calculated based on the number of neighbours and their trust value. The scheme [6] is agent-based method which agents calculates the behaviour of nodes, count all good and bad behaviours. In this model, the probability theory is used to calculate the trust and trust space of three variables including positive trust, negative trust, and uncertainty.

The authors of [7] provided a group-based trust management scheme. In this scheme, all nodes calculate the other member's trust, and cluster head aggregates the trust values and sends to the base station. Then the base station calculates whole group trust value, and assigns one of the three states, trusted, untrusted and uncertain to each group. Finally, cluster head at specified intervals sends the groups' states to cluster heads. In [8] a new scheme was provided for trust calculation in which the cluster heads choose some nodes as surveillance nodes to monitor the cluster nodes' behaviours and calculate their trust and reputation. Using this mechanism, surveillance nodes can identify invalid or wrong data created by compromised nodes.

In [9] provided a trust model based on Bayes theory in which trust calculation consists of two parts, a communication trust which is calculated based on routing information and data trust which is calculated based on successfully received data. In [10] authors used nodes trust and fuzzy logic to create a trusted path between the source and destination nodes, then nodes with the highest trust value are selected to deliver packets. The study of [11] was developed based on D-S theory and fuzzy logic. In this scheme, the trust is calculated based on the observation of neighbour nodes' behaviour and packets sent [12].

3. Proposed Scheme

It is believed that nothing is secured and can be trusted. With enough time and money, attackers will definitely find a way to break and attack any systems. Therefore a clear definition of a trusted system is needed. The process of proposed approach follows four stages: trusted approach, beta distribution, Josang subjective logic and Direct Trust Calculation. Before expressing our trust plan, we outline the assumptions that have been considered for the network. A trusted authority is responsible for:

- A unique identity is considered for each network node (ID_x is the unique ID of node x).
- A random number called s is chosen as the network security key that only network nodes are aware of it.
- For each node such as x a key based on node ID and network security key are made as follows:

$$K_x = SH(ID_x) \tag{1}$$

Where H is the map point hash function and K_x is the unique key of node x. Each node such as node x is preload by unique ID and key before the network development.

3.1 Trust approach

In our proposed approach, a heterogeneous cluster-based wireless sensor network is considered. The initial clustering is performed by any clustering protocol such as leach. Each node after the transaction with another node according to the behaviour of cross-node during the transaction and the quality of service which received evaluates that transaction and considers it as a positive transaction (p) or negative transaction (n). Then, at a specified period time, each node calculates the trust of neighbour nodes according to the number of positive and negative transactions that has stored for each neighbouring node. In the proposed approach the beta distribution and Josang subjective logic used to calculate the trust which explained in next section.

3.2 Beta Distribution

In the theory of probability and statistics, beta distribution is a family of continuous probability distribution which is usually used for continuous random variables in the range [0, 1] and is defined by two parameters α and β. Due to the characteristics of beta distribution, mathematical expectation is as follows:

$$E(b/\alpha,\beta) = \frac{\alpha}{\alpha+\beta} \tag{2}$$

For calculating trust using a beta, the number of interactions with a positive result (p) is attributed to the parameter α and the number of interactions with the negative result (n) is attributed to parameter β. Finally, trust is calculated as follows [13]:

$$T = E(b/\alpha,\beta) = \frac{\alpha}{\alpha+\beta} = \frac{p+1}{p+n+2} \tag{3}$$

3.3 Josang Subjective logic

In Josang subjective logic, a trust is presented in three terms (b, d, u) which respectively shows believe, disbelieve and uncertainty where the condition is b + d + u = 1. Then another parameter as the base rate (a) in the interval [0, 1] enters the previous representation and the quartet (b, d, u, a) is formed. The base rate determines how much uncertainty can be involved in the mathematical expectation of trust level. Mathematical expectation of trust level (the value that is estimated ultimately as the trust level from the trilogy (b, d, u) is considered as follows [14] :

$$E(T) = b + au \tag{4}$$

Values b, d and u can be calculated in different ways; in our approach, these values are calculated as follows:

$$b = \frac{p}{p+n+1} \tag{5}$$

$$d = \frac{n}{p+n+1} \tag{6}$$

$$u = \frac{1}{p+n+1} \tag{7}$$

3.4 Direct Trust Calculation

According to [23], trust can be defined as an entity that always behaves in the expected way for the intended function. Calculating trust of our approach is performed in three steps:

Ttotal: Total trust is calculated based on beta distribution (1) and all interactions between the two nodes are considered.

Tlast: the trust in recent transactions calculated based on Josang subjective logic. For each transaction, a coefficient considered according to the time of transaction, and in specified intervals the recent trust is calculated based on the last transactions. Weighting coefficient of each transaction is calculated according to the following formula:

$$a_i = \frac{1}{\lambda^i} \tag{8}$$

Where i is the past time unit of the transaction, λ is forgetting factor which can be changed according to network conditions and α_i is transaction coefficient that i units of time is passed. After a long interval, the effect of coefficient becomes very low and close to zero, therefore a time window is considered to calculate these coefficients. The size of time sliding window can be changed according to conditions and trust node. For example, if the final value of trust is less than the threshold, or a node in the most recent transactions shows bad behaviour, the size of sliding window is reduced, so the node detected as a misbehaviour. After assigning appropriate coefficient to recent transactions, the recent trust is calculated based on Josang subjective logic.

Tfinal: In this step, the final trust is calculated according to the results of the two previous steps and fuzzy logic. A fuzzy system does not require large computational complexity; therefore, it is appropriate for WSNs.

The membership functions of input parameters are shows in Figure 1.

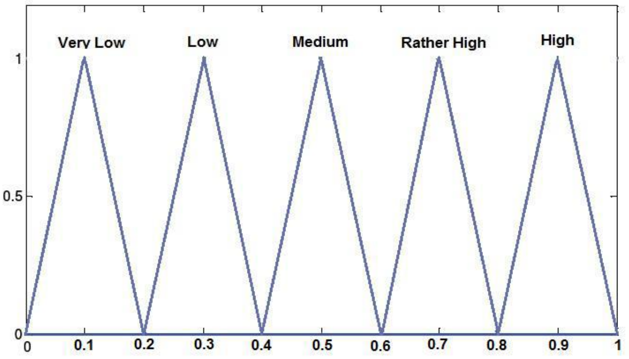

Fig.1. Trust membership function

Fuzzy logic rules considered to calculate the final trust are shown in Table 1. Hence, according to the rules and membership functions built in Fuzzification stage, classical probability values are converted to Fuzzy input values which are usually fuzzy sets.

Table.1. Trust fuzzy logic rules

Ttotal	Tlast	Tfinal
High	High	Exactly Trusted
High	rather High	Trusted
High	Medium	rather Trusted
High	Low	Untrusted
High	very Low	Untrusted
rather High	High	Trusted
rather High	rather High	Trusted
rather High	Medium	rather Trusted
rather High	Low	Untrusted
rather High	very Low	Untrusted
Medium	High	rather Trusted
Medium	rather High	rather Trusted
Medium	Medium	rather Trusted
Medium	Low	Untrusted
Medium	very Low	Untrusted
Low	High	rather Untrusted
Low	rather High	rather Untrusted
Low	Medium	rather Untrusted
Low	Low	Untrusted
Low	very Low	Untrusted
very Low	High	rather Untrusted
very Low	rather High	rather Untrusted
very Low	Medium	Untrusted
very Low	Low	Untrusted
very Low	very Low	Untrusted

The process of calculating trust is also established in the second level of the network between cluster heads and the base station. According to the importance of most communication at this level, the size of slider window is considered smaller which can determine the effect of interactions earlier. In addition, when base station considers a cluster head destructive or its trust level is lower than a threshold, it is quickly removed and placed on a blacklist.

4. Reputation Calculation

The reputation of each node is the outcome of trust aggregation of other nodes to the target node. Nodes within each cluster periodically send trust values in their trust table to the cluster head. When the cluster head receives a certain number of comments about a node, it updates the reputation of that node in its trust table based on these comments. The effect of each node's comment in the aggregation of comments depends on the reputation in the cluster head reputation table and is calculated based on the following formula:

$$Rep_x = a_y T_{y\to x} + a_k T_{k\to x} + a_l T_{l\to x} + \cdots = \sum_{i=\{y,k,l,\dots\},i\neq \mathrm{x}}^{cnt} a_i \; T_{i\to \mathrm{x}} \quad \text{where } \sum_{i=1}^{cnt} a_i = 1 \tag{9}$$

where, Rep$_\mathrm{x}$ determines the reputation of node x, $T_{i\to x}$ expresses the trust value of node i to node x and i is a set of nodes that commented about node x. cnt is the total number of nodes that commented on node x and α_i is weighting coefficient of each comment and shows the effect of each node's comment in the calculation of reputation of node x. For example, weighted coefficient of node y comment is calculated as follows:

$$a_y = Rep_y / \sum_{i=\{y,k,l,\ldots\}}^{cnt} Rep_i \qquad (10)$$

Cluster head uses calculated reputation values in important processes such as data aggregation and new cluster head selection for updating the reputation of each node. Moreover, the nodes in the cluster can also use these values as indirect trust. Cluster heads prepare a list of untrusted nodes based on their reputation table and broadcast in the cluster periodically so other nodes are more careful to communicate with them.

5. Cluster Head Selection

The new cluster head is selected periodically by the current cluster head. The process of the cluster head selection in our approach is performed in two steps:

Screening: First, the cluster head according to its reputation table selects node among the nodes in the cluster whose reputation value is greater than the threshold, and these nodes will enter the second step as candidate nodes to be cluster head. Trust threshold can be changed according to network conditions and is usually more than 0.5.

Cluster head selection with fuzzy approach: as regards goal of our approach is improve network security, and energy which always be one of the most important parameters in WSNs, the remaining energy of node and the number of trusted neighbors were considered as fuzzy system input. The membership functions of input parameters are shows in Figures 2 and figure 3.

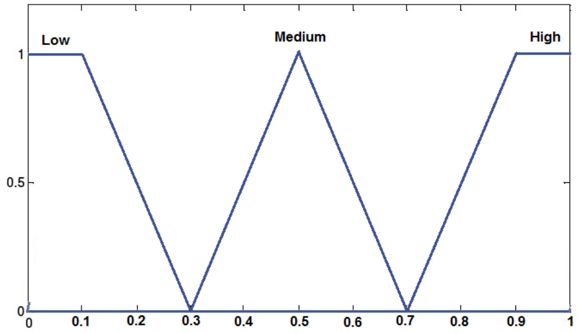

Fig.2. Membership Function of Energy

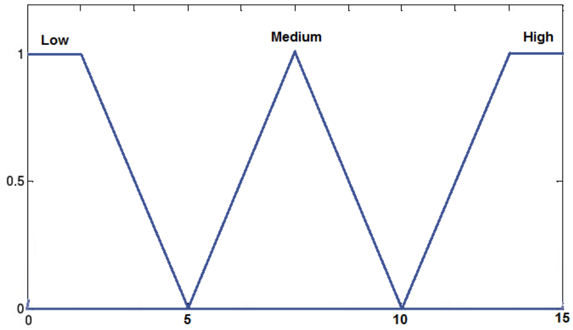

Fig.3. Membership function of Trusted Neighbor Nodes

Fuzzy logic rules considered for calculate cluster head probability and trusted neighbors to cluster head selection are shown in Table 2.

Table 2. Cluster head selection fuzzy logic rules

Energy	Become Cluster Head Probability	Number of Trusted Neighbors
High	Highest	High
High	Rather High	Medium
High	Low	Low
Medium	High	High
Medium	Medium	Medium
Medium	Low	Low
Low	Rather Low	High
Low	Low	Medium
Low	Lowest	Low

6. Analysis of proposed scheme

In this section, experimental results of the proposed approach are explained. Firstly, an analysis of most common attacks against the trust systems is provided and then, to verify the performance of proposed approach in the defined scenario, simulation results are shown.

6.1 Security Analysis

On-Off Attack: In this attack, the malicious node shows a good behavior strategically for a period of time to enhance its reputation and attract the trust of other nodes [15, 16]. Then it begins to misbehave. The trust system will not repel this attack for short time and at this time can cause great harm to the network. Then shows normal behavior to keep its trust and reputation level [17, 18]. This scheme is resisted against on-off attack because of the effect of time and calculation of trust based on the last interactions. If a node after the increase of trust value wants to misuse this behavior, once it shows an abnormal behavior for a short period, the recent trust and as a result, the final trust to this node will be decreased significantly.

Reputation squeeze Attack: In this attack, a node with good behavior in low-value interactions gains a high reputation, then in high-value interactions shows bad behavior [19]. For example, a malicious node shows good behavior in normal interactions within the cluster and after increasing its reputation in the cluster uses this reputation in important processes such as data aggregation and cluster head selection. In this method, because of aggregation of comments of all nodes in important processes such as cluster head selection, the effect of an outlier comment will be reduced. In addition, if a high reputation of a malicious node is effective in the selection or deselecting of a cluster head or even leads to select the malicious node as a cluster head, the malicious node quickly identified and will be removed completely from the network.

Re-entry Attack: In this attack, the malicious node to remove its bad record, after a period activity reenter as a new node to the network [16]. This malicious node should acquire a new identity for itself or forge it. In our approach there is no possibility to access or forge a new identity due to network security key and the unique key of each node that has been already preload by a trusted authority in network nodes.

Unfair rating Attack: In In this attack, the malicious node provides untrue and unfair advice about other nodes in the network [20]. Bad mouthing attack is a common type of this attack which the malicious node shows the trust level of a specific node in the network lower than real [21]. Given the weighting of each node's comment based on its reputation in the reputation table of the cluster head, the effect of the malicious node's comment would be negligible in our approach. If the unfair rating is provided by a known and trusted malicious node, the effect of this comment will be automatically removed due to the comments aggregation of all nodes in processes such as reputation calculation and cluster head selection. In addition, because the indirect trust is not calculated by the nodes itself, which calculated by cluster headed, the unfair advice of a malicious node has no effect on the working process of cluster nodes.

Collusion Attack: This attack occurs when several malicious nodes cooperate to indicate the trust level of a node unreal and provide untrue and unfair recommendations about that node [15]. our approach is vulnerable to this attack if a large number of nodes participating in the collusion process and the reputation values of all of nodes will be higher than cluster head`s reputation table. It should be considered that these attack when occur that a large number of cluster nodes which have the network security key and necessary conditions, Being malicious from the beginning. In addition, the attacker can capture a large number of nodes and gain the control of the nodes and the cluster, which by using discrete logarithm in the proposed approach it is impossible to obtain the main secret of the network.

Sybil Attack: In this attack, a malicious node has created several fake identities and uses them to deceive the trust system [22]. This attack due to the use of the unique key ID_x and network security key in the process of authentication is avoided by proposed approach.

6.2 Performance Analysis

In this section, we evaluate the performance of our proposed scheme in MATLAB. In these scenarios, 100 nodes are randomly distributed in a 100×100 M2 network. The parameters values that consider for simulation are shown in Table 3.

Table 3. Cluster head selection fuzzy logic rules

Parameters	Values
Initial reputation values	0.5
Base rate	0.5
Time slider windows size	5
Forgetting factor	0.5
Reputation threshold	0.65

The simulation was performed for 25 rounds, Figure 4 shows 100 nodes with their reputation values and selected cluster heads. As you see in Figure 4 the trust values of selected cluster heads are more than threshold value and all of them have the most trusted neighbours. Also simulation result shows that the proposed scheme prevents untrusted nodes or nodes with low trust value from becoming cluster head.

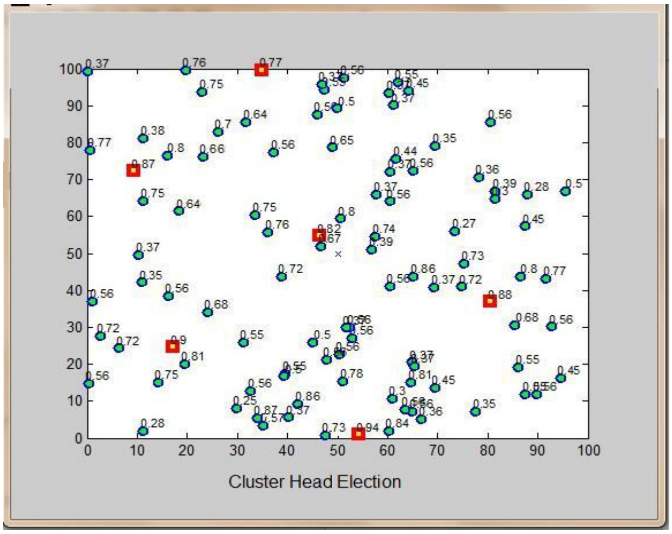

Fig.4. Cluster Head selection

7. Conclusions

In this paper, the strengths and weaknesses of the trust systems have been reviewed and then a new trust approach for wireless sensor networks was suggested which showed simplicity, high flexibility and it’s resistant to various attacks. Our approach composed of three phases. Firstly assumption defined and trust approach described. Then reputation calculation introduced and cluster head selection explained. Simulation results show that the proposed approach prevents untrusted nodes in the network from becoming cluster head. For future work can use cluster head instead of the node to exchange their reputation and take account different parameters in calculating of reputation values.

References

[1] T. Bin, Y. YANG, L. Dong, LI. Qi, XIN. Yang, "A security framework for wireless sensor networks," The Journal of China Universities of Posts and Telecommunications 17, 2010, pp.118-122.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] MK. Jain, "Wireless sensor networks: Security issues and challenges," International Journal of Computer and Information Technology 2.1, 2011, pp.62-67.

[3] V. Umarani, KS. Sundaram. "Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks," 2013.

[4] S. Ganeriwal, L.K. Balzano, M.B. Srivastava, "Reputation based framework for high integrity sensor networks," Proceedings of the 2nd ACM Workshop on Security of adhoc and Sensor Networks, 2004, pp.66–77.

[5] Z.Yao, D.Kim, Y.Doh, "Parameterized and localized trust management scheme for sensor networks security," IEEE International Conference on Mobile adhoc and Sensor Systems, MASS, 2008, pp.437–446.

[6] H. Chen, H.Wu, X.Zhou, C.Gao, "Agent-based trust model in wireless sensor networks," 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel Distributed Computing, 2007, pp. 119–124.

[7] R.A. Shaikh, H.Jameel, B.J.d’Auriol, H.Lee, S.Lee, Y.J.Song, "Group-based trust management scheme for clustered wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems 20 (11), 2009, pp.1698–1712.

[8] Y.Zhou, T.Huang, W.Wang, "A trust establishment scheme for cluster-based sensor networks," 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, pp. 1–4.

[9] Z.Liu, Z.Zhang, S.Liu, Y.Ke, J.Chen, "A trust model based on Bayes theorem in WSNs," 7th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM, 2011, pp. 1–4.

[10] T.K. Kim, H.S. Seo, "A trust model using fuzzy logic in wireless sensor network," Proceedings of World Academy of Science Engineering and Technology, 2008, pp. 63–66.

[11] R.Feng, X.Xu, X.Zhou, J.Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D–S evidence theory",Sensors 11(2), 2011, pp. 1345–1360.

[12] Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. "Management and applications of trust in Wireless Sensor Networks, A survey," Journal of Computer and System Sciences 80.3, 2014, pp. 602-617.

[13] WT. L, J. Patel, NR. Jennings, and M. Luck, "Coping with Inaccurate Reputation Sources:Experimental Analysis of a Probabilistic Trust Model," Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems, 2005, pp. 997-1004.

[14] A. Josang, E.Gray, M. Kinateder, "Simplification and Analysis of Transitive Trust Networks," Web Intelligence and Agent Systems Journal, Vol. 4, No. 2, 2006, pp. 139-161.

[15] FG. Marmol, and GM. Pérez, "Security threats scenarios in trust and reputation models for distributed systems," Computers & Security 28.7, 2009, pp. 545-556.
[16] Y. Yu, K. Li, W. Zhou, P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of network and computer applications 35.3, 2012, pp. 867-880.
[17] Y. Sun, Z. Han, KJR. Liu, "Defense of trust management vulnerabilities in distributed networks," Communications Magazine, IEEE 46.2, 2008, pp. 112-119.
[18] H. Yu, Z. shen, C. Miao, C. Leung, D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proceedings of the IEEE 98.10, 2010, pp. 1755-1772.
[19] B. Khosravifar, J. Bentahar, M. Gomrokchi, R. Alam, "CRM: An efficient trust and reputation model for agent computing." Knowledge-Based Systems 30, 2012, pp. 1-16.
[20] FG. Zhang, "Preventing recommendation attack in trust-based recommender systems," Journal of Computer Science and Technology 26.5 , 2011, pp. 823-828.
[21] Y, Yang, Q. Feng, YL. Sun, Y.Dai, "Reptrap: a novel attack on feedback-based reputation systems," Proceedings of the 4th international conference on Security and privacy in communication netowrks. ACM, 2008.
[22] D.Ingram, "An evidence based architecture for efficient, attack-resistant computational trust dissemination in peer-to-peer networks," Trust Management. Springer Berlin Heidelberg, 2005. pp. 273-288.
[23] D. Grawrock, Dynamics of a Trusted Platform: Intel Press, 2009

Authors’ Profiles

Mohsen Salehi received MSc Degree in Computer Engineering from Imam Reza International University, Iran, in 2014. He received the B.S. degree in computer engineering from Shahrood University. He has published several researches Paper in Computer science Field. His research interest includes Data Mining, Network, Security, image processing and artificial intelligence.

Jamal Karimian (born September 17, 1989) is an Iranian Software Engineer. He received his Master degree from Imam Reza University in Mashhad in 2014 and has been researching in various fields of computer science such as data mining, artificial intelligence and Network. He has a lower academic level He spent his time at the Montazeri Shahid University and Jahad Daneshgahi, and became one of his most distinguished students.

How to cite this paper: Mohsen Salehi, Jamal Karimian," A Trust-based Security Approach in Hierarchical Wireless Sensor Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.6, pp. 58-67, 2017.DOI: 10.5815/ijwmt.2017.06.06