Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 5, May -2016

Trust Management systems in Wireless Sensor Networks: a Survey

Megha Shah[1], Rituparna Sarma[2]

[1]Computer science & Engineering, Parul Institute of Engineering & Technology
[2] Faculty of Computer science & Engineering, Parul Institute of Engineering & Technology

Abstract — *A Wireless Sensor Network (WSN) consists of autonomous sensor nodes that are used to monitor physical and environmental conditions like temperature, pressure etc. Due to the inherent limitations of sensor networks, commonly used security mechanisms are hard to implement in these networks. For this very reason, security becomes a crucial issue in WSNs. Recently, a trust based schemes are introduce as an effective security mechanisms. In this paper, we present a survey on various trust models. Some security attacks on trust models are also introduce in this paper and based on the attacks we analyze the efficiency of existing schemes. Finally, we conclude some unsolved issue in trust based schemes in WSNs.*

Keywords- *Wireless Sensor Networks, Trust Management system, Trust Models, Trust, Reputation, Security Attacks*

I. INTRODUCTION

Wireless sensor networks (WSNs) have gained worldwide attention in recent years. WSNs are distributed autonomous sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user [1]. Smart sensor nodes are low power devices equipped with one or more sensors, memory, processor, a power supply, a radio, and an actuator [2].

Wireless sensor networks have to be secured from various attacks especially at unfriendly situations because data can easily be attacked by the attackers [3]. Due to the inherent limitations of sensor networks, commonly used security mechanisms like key management [4], authentication [5], cryptography [6], etc are hard to implement in these networks. For this very reason, security becomes a crucial issue and these networks face a wide variety of attacks such as denial of service (DoS) attack, wormhole attack, black hole attack, routing table overflow and poisoning attack, packet replication attack, gray hole attack and modification of packets attack etc.

Traditional security mechanisms such as authentication, encryption and key cryptography are not suitable for WSN as these mechanisms assumes that all participating nodes are cooperative with each other and trusted and also require more computation, communication and storage. These algorithms are incapable to counter nodes misbehaving attacks.

For securing WSN, the trust and reputation based schemes are proved to be more robust against node misbehavior attacks. Trust based security is a new way of providing security without using traditional approaches.

Trust in the wireless communication networks may be defined as degree of reliability of other nodes performing actions [7, 8]. Trust between the nodes in maintained by recording the transactions of a node with other nodes in the network, either directly or indirectly. A trust value will be calculated from the record that aids sensor nodes to deal with uncertainty about the future actions of other nodes. Trust based approaches are very useful to deal with node misbehavior.

Reputation systems provide a way for building trust through social control by utilizing community based feedback about past experiences of nodes to help making recommendation and judgment on quality and reliability of the transactions.

Some trust and reputation based scheme are developed in MANET [9, 10] but they are not implemented in WSNs because limitations of resources of the sensor nodes.

In WSN a distributed Reputation- based Framework for Sensor Networks (RFSN) [11] is first proposed for WSNs. Two key building blocks of RFSN are Watchdog and Reputation System. Watchdog is used for monitoring communication behaviors of neighbor nodes. Reputation System is used for maintaining the reputation of a sensor node. The trust value is calculated based on the reputation value. However, in RFSN, only the direct trust is calculated while the recommendation trust is ignored. A Parameterized and Localized trust management Scheme (PLUS) is proposed in [12]. In PLUS, both personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. Whenever a judge node (the node which performs trust evaluation) receives a packet from suspect node (the node which is in radio range of the judge node and will be evaluated), it always check the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviors or not. Therefore, suspect node may get unfair penalty.

Another similar trust evaluation algorithm named as NBBTE (Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm) is proposed based on behavior strategy banding D-S belief theory [13]. NBBTE algorithm is first algorithm which establishes various trust factors depending on the communication behaviors between two neighbor nodes. Then, it applies the fuzzy set theory to calculate the direct trust values of sensor nodes. Finally, considering the recommendation of neighbor nodes, D-S evidence theory method is adopted to obtain integrated trust value instead of simple weighted average one. NBBTE is the first proposed algorithm which establishes various trust factors depending on the communication behaviors to evaluate the trustworthiness of sensor nodes.

The purpose of this paper is to highlight trust models for WSNs. It is known that WSNs are energy constraint and vulnerable to malicious attacks. This paper is organized as follows: In Section II, we describe trust management systems, in section II, we describe the attacks on WSNs, and in section IV we analyze and summarize trust models and applications of them in WSNs. Finally, Section V gives the conclusions and open research problems.

II. OVERVIEW OF TRUST MANAGEMENT SYSTEM IN WSNs

To develop a robust and secure Trust Management system for WSNs, it is important to have a clear Understanding of TM. According to Zheng and Holtmanns [14], TM addresses managing trust relationships, such as information collection, to make decisions related to trust, assessment of the criteria related to the trust relationship, and observation and reassessment of existing relationships. Autonomic TM [15] includes four aspects:

- Trust establishment: the process of establishing a trust relationship between communicating pairs.
- Trust monitoring: the process of observing and recording performance or behavior of the trustee by the trustier or by a delegate of the trustier.
- Trust assessment: the evaluation process of trustworthiness of the trustee by the trustier or by a delegate of the trust or based on the recorded information.
- Trust control and re-establishment: On the basis of the trust evaluation, trust relationships are re-established, or corresponding measures are taken to control trust relationships.

Trust management deals with monitoring the performance/ behavior of nodes and recording it; estimating the trust and establishing trust relationships; managing trust relationships, Trust Estimation rules and policies; assisting security services, such as access control, key management and misbehavior detection (Figure 1).

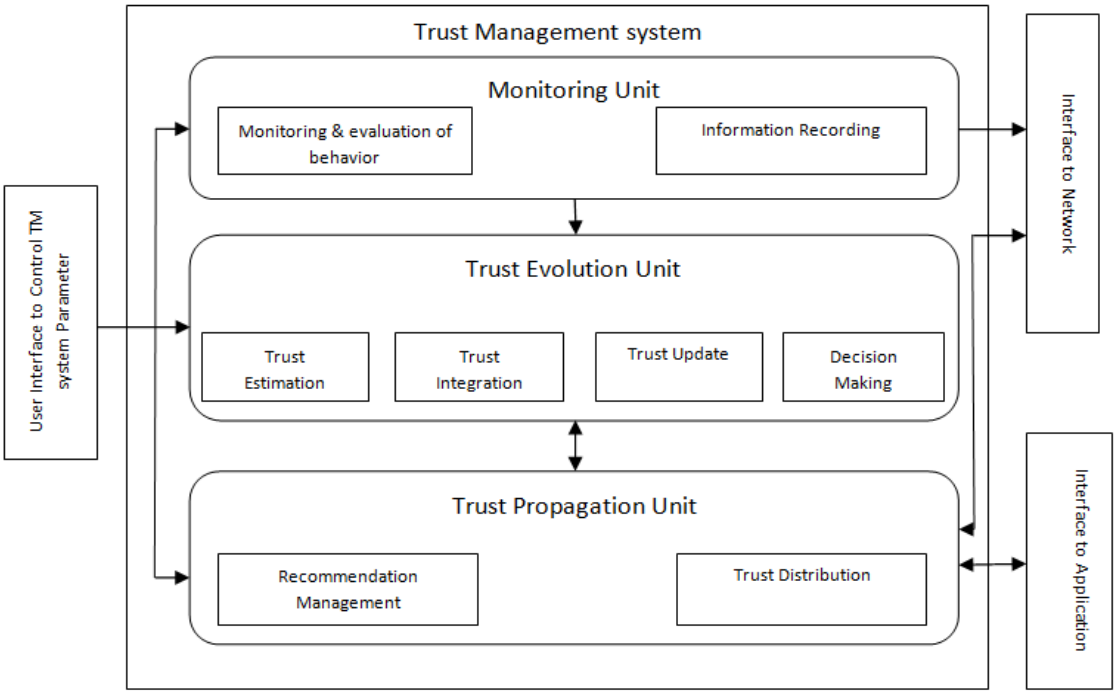

Figure 1. Basic element of Trust management System

Functions of each of the blocks

- Monitoring and learning: Monitor and learn node behavior/performance and provide input to the trust evaluation unit. This is connected to a network interface to collect information about nodes.

- Trust evaluation: This is a central unit of the TM system, which performs estimation and integration of trust and reputation values, decision-making trust value quantization, and information aging, and so on. It provides output to the recommendation management unit.
- Recommendation management: This deals with the distribution and reception of recommendations (trust values). In addition, it provides trust values of nodes for various applications.

The major challenge faced by wireless sensor networks is security. Because of dynamic and collaborative nature of sensor networks, to deal with this issue, a trust model is required to find malicious, selfish and compromised nodes by evaluating trust worthiness sensors from the network. It supports the decision making processes in wireless sensor networks such as key-distribution, cluster head (CH) selection, data aggregation, routing and self reconfiguration of sensor nodes.

In wireless sensor network, trust specifies the reliability or trust worthiness of sensor node. In general, trust may be classified as behavioral or computational trust based on where it is used. Behavioral trust defines trust relations among people and organizations. Computational trust defines trust relation among devices, computers, and networks.

Trust can be direct trust or indirect trust. Direct trust specifies the direct observations of one node to another node and called as first hand information. Indirect trust specifies the indirect observation of sensor nodes and called as second hand information. The trust values calculated between nodes are based on their cooperation in routing messages (packets sending) to other nodes in the network which is termed as communication trust. The trust value calculated is based on the actual sensed data of the sensor nodes in wireless sensor networks is known as data trust.

In wireless sensor networks, trust model specifies plays an important role in identifying misbehavior nodes and providing collaboration among trustworthy nodes. It improves the lifetime of networks. The model is capable of capturing and distributing feedbacks about current interactions among nodes and stores the trust information for future. It also uses feedback to guide trust decisions. Based on trust information, it may be classified as centralized, distributed and hybrid Model. These models are introduced in [16].

In the centralized trust model, trust is mainly based on the provision of a valid certificate assigned to a target node by a centralized certification authority or by other trusted issuer. In distributed trust model, every node locally calculates the trust values of all other nodes in the network that increases the computational cost. Also each node needs to maintain an up-to-date record about the trust values of the entire networking in the form of a table. Hybrid trust model contains the properties of both centralized as well as distributed trust management approaches. The main objective of this approach is to reduce the cost associated with trust evaluation as compared to distributed approaches.

III. VARIOUS SECURITY ATTACKS ON TRUST MODELS

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.
There are several attacks on trust models. Some of the attacks are introduce in paper [17].

Sybil attack: In Sybil attack, malicious nodes can create several fake IDs, then emulate or impersonate different nodes in the network. The Sybil nodes can manipulate there commendations and promote themselves as trust nodes.

DoS attack: In DoS attack, malicious nodes send misleading information, e.g., misleading recommendations, as much as possible to consume large amount of computing resources.

Bad mouthing attack: In this attack model, malicious nodes intentionally give dishonest recommendation for neighbor nodes, even if the neighbor nodes are normal ones. Thus, recommendations under bad mouthing attack cannot reflect their al opinion of their commander.

On-off attack: In this type of attacks, malicious nodes can opportunistically behave good or bad. Thus, malicious nodes can remain trusted while behaving badly.

Conflicting behavior attack: In this attack, malicious nodes behave differently towards different nodes. For example, malicious nodes can give good recommendations about node A to node B, and give bad recommendation about node A to node C. This way, the conflicting recommendations about the node A can confuse the trust model to evaluate trust worthiness of node A.

Collusion attack: Collusion attacks are engendered by more than one malicious node collaborating and giving false recommendations about normal nodes. Collusion attacks are much more destructive than above mentioned attack models which implemented by one malicious node.

IV. TRUST MODELS AND ITS APPLICATIONS IN WSNS

4.1 TRUST MODELS

4.1.1 Distributed Trust Model

An Efficient Distributed Trust Model is proposed in [18] for Wireless Sensor Networks proposed to an efficient and attack-resistant trust model. In this model first, according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. Furthermore, trust reliability and familiarity are defined to improve the accuracy of recommendation trust. The proposed EDTM can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more effectively.

4.1.2 Multiple-level trust management

A novel multiple-level trust management framework for wireless sensor networks is proposed in [19]. In ML-Trust three levels of trust are used to establish trustworthy relationships among nodes for their cooperation, namely, (1) a subjective trust, which is defined as belief and is proposed with respect to three aspects: past judgments, witness evidence, and capacity evaluation; (2) an objective trust, which is defined as reputation and is proposed with two factors, number of functioning communities and weighted judgments by rating nodes' reputations, being introduced in reputation rating, and with several rules and fraud factor tests being given to prevent reputation rating from malicious attacks, and (3) the recommended trust method, which is proposed to obtain trustable impressions from strange recommendations with, in connection, several consistency factors being presented to determine the trustworthiness of a recommendation. Ml-Trust is proving robust against malicious behavior node.

4.1.3 Risk-aware Reputation-based Trust (RaRTrust) model

A Risk-Aware Reputation-Based Trust Management in Wireless Sensor Networks is proposed in [20]. Risk-aware Reputation-based Trust (RaRTrust) model uses both reputation and risk to evaluate trustworthiness of a sensor node. Trust value computation is based on two components: reputation evaluation and risk evaluation. Reputation evaluation is based on direct and/or indirect observations, and represents the accumulative assessment of the long-term behavior. Risk evaluation is based on interaction-derived information that is the self-opinion from the direct interactions which is reliable and self-determined and represents the opinion of the short-term behavior. Risk evaluation is a very helpful component to build the trust model that effectively deals with conflicting behaviors node Risk evaluation is used to deal with the dramatic spoiling of nodes, which makes RaRTrust robust to on–off attack and differ from other trust models based only on reputation. This paper contributes to model the risk as opinion of short-term trustworthiness combining with traditional reputation evaluation to derive trustworthiness in WSNs.

4.1.4 Lightweight Trust Model

Lightweight Trust Model for Clustered WSN (LTM) is proposed in [21]. LTM calculates direct and indirect trust. Direct trust is evaluated by monitoring some events, called trust metric, which is divided into two groups with priority. The trust relationship is classified into two different sheets: Intra cluster and Inter cluster trust formation. In the former, trust relationship is calculated among *CM*s (Direct trust), and between *CH* and *CM*s (Indirect trust). Our trust model effectively recognizes the malicious nodes by the final updated trust values between dealing nodes.

4.1.5 Agent-based Trust management model

In Agent-based Trust management model for WSNs (ATSN) [22] the agent nodes broadcast the encrypted trust values to its neighbors. The drawback of ATSN was that it uses promiscuous mode of operation to monitor the behavior of its neighbor. The drawback of the promiscuous mode of operation is the demand for Omni-directional transceivers and consumption of more energy as the nodes need to remain in the wakeup state for longer duration.

4.2 APPLICATIONS OF TRUST IN WSNs

4.2.1 Secure Data aggregation

Trust management is useful for data aggregation. Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks [23] proposed a trust based scheme for data aggregation. In the proposed improved protocol, consider a cluster that is composed of a group of sensor nodes. In order to combine first-hand and second-hand information to calculate nodes' reputation and trustworthiness, the nodes can cooperate with neighboring nodes in the same group to exchange the table of their observation results. According to the received tables of observation results, each node can calculate neighboring nodes' reputation and trust value, and judge whether a nodes is compromised or not. The proposed method introduces the relationship between nodes and the strength of the ties into the evaluations of nodes' trustworthiness and improves the efficiency by using second-hand information coming from neighboring nodes.

4.2.2 Secure routing

In ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks [24] energy efficient routing scheme is proposed by using the trust model. ETARP designed for energy efficiency and security for wireless sensor networks (WSNs). ETARP attempts to deal with WSN applications operating in extreme environments such as the battlefield. The key part of the routing protocol is route selection based on utility theory. The concept of utility is a novel approach to simultaneously factor energy efficiency and trustworthiness of routes in the routing protocol. ETARP discovers and selects routes on the basis of maximum utility with incurring additional cost in overhead compared to the common AODV (Ad-Hoc On Demand Distance Vector) routing protocol. It uses the AODV routing protocol scheme but it replace the " hop count" field of RREQ and RREP packet to the " Energy count". The utility or preference designated for a route is related to both energy cost and security level (trustworthiness). Bayesian Network checks that whether the node is safe or risky. Through simulation's results it shows that the energy efficiency performance and safety performance of ETARP is evaluated.

Trust Aware Routing Framework for WSNs (TARF) [25] is a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. Energy and trust watcher are used in TARF. Energy Watcher on a node monitors energy consumption of one-hop transmission to its neighbors and processes energy cost reports from those neighbors to maintain energy cost entries in its neighborhood table; its Trust Manager also keeps track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its locality table.

A collaborative lightweight trust-based (CLT) routing protocol [26] is proposed because earlier security solutions aimed at thwarting different types of malicious threats but failed to consider the resource constrained nature of sensor nodes. The stringent resource constraints of WSNs require a lightweight trust-based routing scheme.

The CLT protocol was proposed to meet the following design objectives:

• To improve the packet delivery ratio by designing an efficient trust management scheme,

• To minimize the memory consumption by representing the trust efficiently, and

• To minimize the energy consumption significantly by avoiding promiscuous mode of operation.

Proposed CLT protocol is for trust establishment in WSNs. Like 2-ACKT protocol, CLT also used 2-ACK routing protocol to identify the sponsor and third party to derive the direct trust. In addition to the direct trust, the CLT protocol derived the trust through recommendation from the neighbors. The indirect trust was used to generate a trust consistent in the network. CLT also employed a novel trust counselor to warn and improve the trust of the nodes present in the alternate path namely, sponsor and third party. It used a sliding time window mechanism to derive the historical trust of the neighbors. It used aging factor to remember the bad behavior of a node for longer duration.

4.2.3 Malicious attack detection

Trust Management for Defending On-off Attacks [27] is introducing for on-off attack. They have demonstrated how predictability trust with sliding windows can allow for flexible design in which a system designer is able to decide the number of opportunities a node should be allowed before being eliminated from the system. This allows the designer to choose an acceptable level of Off-to-On ratio to trade-off security for performance.

In order to avoid selfish nodes that are likely to refuse forwarding packets, a Data centric Dumpster Shafer theory based Selfishness Thwarting via Trust evaluation is proposed in [28]. D2S2T2 defines trust in regard to forwarding and in regard to recommendations. $TF+\ i\ j$ and $TF-\ i\ j$ are defined to reflect how much node i trusts node j to forward or not forward node i's packets, respectively. Then, node i can use a threshold heuristic to treat node i as selfish ($TF-\ i\ j \geq S\ T$) or non-selfish ($TF+\ i\ j \geq S\ T$), where $S\ T \in (0.5, 1]$ is a selfishness threshold. In most selfishness detection mechanisms, in order to speed up detection of selfishly misbehaving nodes, node shares their opinions with neighbor nodes in the form of recommendation messages. However, false recommendations are always ignored. Therefore, in D2S 2T2, trust associated with recommendation message is diminished. D2S 2T2 cannot only detect selfish nodes, but also effectively control the impact of false recommendations to make the system more robust against malicious attacks.

V. CONCLUSION

In this paper we study security and security attacks in WSNs. We have seen that the traditional schemes are not useful in WSNs that's why the trust based schemes are introduce in recent years. We study the various trust models and its application. Trust models are becomes useful to detect malicious and selfish nodes which are not detected by the traditional techniques.

Based on the above discussed trust management systems we conclude that:

Trust management systems are useful for malicious nodes detection but it has to be more robust against various security attacks.

Some trust based routing protocols need to develop to protect WSNs from routing attacks like DoS attack, Sybil attack, and collusion attack.

Most trust management mechanisms evaluate trustworthiness based on interactions among sensor nodes while pay little attention to privacy preserving in the computation of trust value.
In future we can develop a scheme to calculate trust threshold value and also develop a trust based schemes for other wireless sensor networks like heterogeneous WSNs, spare WSNs, dynamic WSNs and so on.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Science direct computer networks, 2292–2330, 2008.
[2] Ado Adamou, Abdelhak gueroui, Nabila labraoui, blaise omer yenke, "concepts and evolution of research in the field of wireless sensor networks", International Journal of Computer Networks & Communications, Vol.7 No.1, pp. 81-98, 2015.
[3] Abdul Wahid, Pavan Kumar, "A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network", International Journal for Innovative Research in Science & Technology, Volume-1 issue-8, pp. 189-196, 2015.
[4] Sarmistha Neogy, "Security Management in Wireless Sensor Networks".
[5] ManikLalDas, "Two-Factor User Authentication in Wireless Sensor Networks", IEEE transactions on wireless communications, VOL-8, NO- 3, pp. 1086-1090, 2009.
[6] Arvindpal S. Wander, Nils Gaura, Vipul Gupta, "Energy analysis of public key cryptography for wireless sensor network"; Proceedings of the 3rd IEEE Int'l Conf. on Pervasive Computing and Communications;2005.
[7] Farruh Ishmanov, Aamir Saeed Malik, Sung Won Kim and Bahodir Begalov; "Trust management system in wireless sensor networks: design considerations and research challenges"; Wiley online publication; 2013.
[8] Shenyun Che, Renjian Feng, Xuan Liang and Xiao Wang; "A lightweight trust management based on Bayesian and Entropy for wireless sensor networks"; Willey online publication; 2015
[9] Arijita Banerjee, Sarmistha Neogy, Chandreyee Chowdhury," Reputation Based Trust Management System for MANET" , 2012 Third International Conference on Emerging Applications of Information Technology, pp. 376-381, 2012.
[10] Kannan Govindan, Prasant Mohapatra,"Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", VOL- 14, NO.-2, pp. 271-298, IEEE communications surveys & tutorials, 2012.
[11] S.Ganeriwal, L.K.Balzano and M.B.Srivastava, Reputation-based Framework for High Integrity Sensor Networks, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Vol.4, No- 3, 2004.
[12] Z.Yao, D.Kim and Y.Doh, PLUS: Parameterized and Localized trust management Scheme for sensor networks security, IEEE International Conference on Mobile Ad hoc and Sensor Systems(MASS), pp. 437-446, 2008.
[13] 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, 2011.
[14] Zheng Y, Holtmanns S. Computer Security and Politics: Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, 2008.
[15] Zheng Y. Autonomic trust management in a component based software system, IEEE Transactions on Dependable and Secure Computing, 2010.
[16] V Uma Rani, K. Soma Sundaram, "Review of Trust Models in Wireless Sensor Networks", International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol-8, No-2, 361-367, 2014.
[17] Guangjie Han, Jinfang Jiang, LeiShu, JianweiNiu, Han-ChiehChao, "Management and Applications of Trust in Wireless Sensor Networks: A Survey", Journal of Computer and System Sciences, 2013.
[18] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Mohsen Guizani; "An Efficient Distributed Trust Model for Wireless Sensor Networks"; IEEE Transactions on Parallel and Distributed Systems; VOL. 0, NO. 0, 1-11, 2014.
[19] Bo Zhang, Zhen hua Huang, Yang Xiang,"A novel multiple-level trust management framework for wireless sensor networks", Science direct, pp. 45-61, 2014.
[20] Nabila Labraoui, Mourad Gueroui, Larbi Sekhri, "A Risk-Aware Reputation-Based Trust Management in Wireless Sensor Networks", Springer Science Business Media New York, 2015.
[21] Moutushi Singh, Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Koushik Majumder, Sudhabindu Ray, and Subir Kumar Sarkar, "Lightweight Trust Model for Clustered WSN", Springer International Publishing Switzerland, 765-773, 2015.
[22] Hu, J., Chen, H., & GAO, C; "Agent-based trust management model for wireless sensor network", in 2nd international conference on multimedia and ubiquitous engineering, pp. 150-154, 2008.
[23] Yun Liu, Chen-xu Liu, Qing-An Zeng, "Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks", Springer Science Business Media New York , 2015
[24] Pu Gong, Thomas M. Chen, and Quan Xu;" ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks"; Hindawi Publishing Corporation Journal of Sensors; Volume 2015, 2015.

[25] M. PRASANTHI, GOVARDHAN REDDY KAMATAM; "Design and Implementation of TARF: A Trust Aware Routing Framework for WSNs"; International journal of advanced technology and innovative research; VOL. 9, NO. 2, pp. 184-197, 2014.

[26] X. Anita, M. A. Bhagyaveni, J. Martin Leo Manickam; "Collaborative Lightweight Trust Management Scheme for Wireless Sensor Networks"; Springer Science+Business Media New York, 2014.

[27] Younghun Chae, Lisa Cingiser DiPippo, Yan Lindsay Sun," Trust Management for Defending On-off Attacks", IEEE Transactions on Parallel and Distributed Systems, pp. 1-14, 2014.

[28] J.Konorski, R.Orlikowski, "Data Centric Dempster Shafer Theory Based Selfishness Thwarting via Trust Evaluation in MANETs and WSNs", Proceedings of the 3rd international conference on New technologies, mobility and security, 2009.

