IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 54-57
International Conference on Management Practices, Innovations & Research 2019

A Survey on Node Level Trust Management Schemes for Wireless Sensor Networks

[1]Lekhchand Sharnagat, [2]Rajesh Babu, [3]Roshani Talmale
[1]*M.Tech Student, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.*
[2]*Assistant Professor, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.*

Abstract*—*A sensor system will review our health, our home, the streets we follow, the workplace or the industry we work in or even theaircrafts we use, trying to improve our safety. Notwithstanding, the wireless sensor networks themselves are inclined to security attacks. The listof security attacks, in spite of the fact that officially exceptionally long, keeps on enlarging obstructing the development of these networks. Thetrust management schemes comprise of a powerful tool for the detection of unexpected node behaviors either malicious or faulty. In wirelesssensor networks, sensor nodes in the region of interest must report the cognitive process to the sink by sensing, and this report will satisfies thereport frequency necessary by the sink. Inside the domain of system security, we decipher the idea of trust as a connection among entities thattake part in different conventions. Trust relations are focused around confirmation made by the past connections of substances inside aconvention. In wireless sensor network the resource efficiency and reliability of a trust system are the most basic supplies. Due to the lowreliability and high overhead the developed existing trust systems for wireless sensor networks are unable of satisfying these supplies. Thereforethere is need to propose a lightweight and reliable trust system which can efficiently decrease the networking consumption while malicious,selfish and faulty cluster heads and also exceeds the limitations of traditional weighting methods for trust factors in which weights are allocatedsubjectively and also insist less communication overhead and memory.
Keywords*—*Trust Management, Security, Wireless Sensor Networks, Lightweight WSN

I. Introduction

Wireless sensor Networks propose possibly supportive plans for various applications including climate and temperature watching, turnpike traffic breaking down, people pulses detecting, and various other military applications. A genuine element of these frameworks is that sensor hubs in frameworks help each other by passing information, in-network procedure and control parcels beginning with one hub then onto the following. It is normally named an infrastructure-less, self-sorted out, or unconstrained framework. Trust management is major to perceive noxious, egotistical and traded off hubs that have been approved. It has been extensively pondered in various network circumstances, for instance, shared network, peer and inescapable preparing and so on. In any case, truth be told, sensor hubs have compelled resources and other remarkable characters, which make trust management for WSNs increasingly basic and testing. Up to the present, investigate on the trust management parts of WSNs has basically centered around the hub's trust appraisal to update the security and force. The sensible utilization of this technique consolidates the course, information joining and cluster head vote. Clustering calculations can successfully improve the network throughput and adaptability for wireless sensor networks like EEHC, HEED, LEACH [4], and EC [13]. The hubs are gathered into the cluster with the assistance of clustering calculation and inside each cluster, the hub which has high processing force and vitality chose as a cluster head CH). Typically the hubs closer to the base station will be vivaciously loaded.[7] Trust establishment in an assembled domain is of Incredible criticalness. Trust is the longing of one component about the exercises of a substitute. A trust structure enables a CH to perceive defective or noxious hubs inside a gathering, controls the choice of trusted steering hubs through which a cluster part (CM) can send information to the CH. In the midst of intercluster correspondence, a trust system moreover helps in the choice of trusted steering door hubs or other trusted CHs through which the sender hub will advance information to the base station (BS).

A WSN contains battery-power sensor hubs with significantly confined taking care of capacities. With a slight radio correspondence run, a sensor hub remotely sends messages to a base station through a multi-jump way. The advantage of viability and dependability of a trust system are the most essential necessities for WSNs. On the other hand, existing trust systems made for clustered WSNs are unequipped for satisfying these necessities because of their high overhead and low unwavering quality. Furthermore, executing complex trust evaluation figuring's at each CM or CH isn't down to earth. In existing trust components, the trust management

framework assembles remote input and afterward, the reactions from every one of the hubs are amassed to get the overall reputation which can be used to survey the worldwide trust degree (GTD) of this hub. On account of the communicated idea of the WSN condition, it contains a considerable number of undependable or malignant hubs. Analysis from these undependable hubs may realize the off base assessment of input. So a trust framework should be significantly solid to the extent of giving organization in an open WSN environment. [10]

II. Trust Management System

Trust is a critical variable in the choice making procedures of any system where instability is a component. Management System: if a component of the system knows ahead of time the real conduct of their accomplices (e.g. malicious, faulty, and collaborative), it can settle on an impeccable choice. All the components of the network work towards the same objective, and they have not reason or the will to carry on selfishly. On the other hand, a sensor node does not have data with respect to others that will permit it to know ahead of time how a transacting accomplice is going to act. Thusly, there is some data asymmetry that the node must arrangement with. At the point when a sensor node picks an accomplice to team up with, such accomplice should be fair and completely synergistic. Sensor systems can endure the attack of noxious nodes or the presence of flawed nodes. As a result, vulnerability in sensor networks is an issue that must be managed a Wireless Sensor Network must be ready to design itself amid its lifetime in vicinity of exceptional occasions.

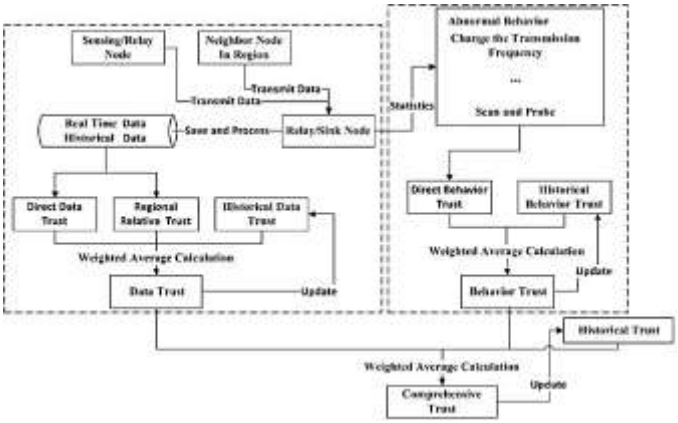

Figure 1. Architecture of Trust Management system

III. Related Work

A.GTMS (Group Based Trust Management Scheme):

Traditional trust schemes for clustered WSNs focus on the trust values of individual nodes but, In GTMS evaluates the trust of group of nodes. This approach gives us the benefit of requiring less memory to store trust records at each Sensor node in the network. GTMS works on two topologies: intragroup topology where distributed trust management approach is used and intergroup topology where centralized trust management approach is adopted. This methodology helps to drastically reduce the cost associated with trust evaluation of distant nodes. GTMS not only provides a mechanism to detect malicious nodes but also provides some degree of prevention mechanism. [9]

Advantages:

1. Scheme is memory efficient and consumes less communication overhead.
2. GTMS uses a hybrid trust management approach, which reduces the cost of trust evaluation.

Disadvantages:

1. Limited work has focused on resource efficiency.
2. Limited work focused on dependability of trust system itself.
3. GTMS relies on broadcast based strategy to collect feedback from the CMs of the cluster, which requires significant amount of resources and power.

B.HTMP (Hierarchical Dynamic Trust Management Protocol):

This trust scheme consider not only quality of service (QoS) trust derived from communication networks, but also social trust derived from social networks to judge if a node is trustworthy to deal with selfish (uncooperative) or malicious nodes. This approach design and validate a hierarchical trust management protocol that candynamically learn from past experiences and adapt to changing environment conditions (e.g., increasing hostility or misbehaving node population) to maximize application performance and enhance operation agility.

This is achieved by addressing critical issues of hierarchical trust management, namely, trust composition, aggregation, and formation. For trust composition, novel social andQuality of Service trust components are considered. For trust aggregation, the best way to aggregate trust (direct vs. indirect trust evaluation) and propagate trust (trust data collection, dissemination and analysis) for each individual trust component, and ascertain protocol accuracy by means of a novel model-based analysismethodology.[1]

Advantages:
1. This scheme design and validate hierarchical trust management protocol that can dynamically learn from past experiences and dynamically adapt to changes in the environment.
2. Subjective trust is validated against the objective trust.

Disadvantages:
1. Implementing such complex trust evaluation scheme at each CM of the cluster is unrealistic.
2. Very less work has been focused on resource efficiency and dependability.
3. More Memory space required for storing the trust values.

C. TCHEM (A Trust Based Cluster Head Election Algorithm):

Its framework is useful for cluster-based wireless sensor networks and, a mechanism that reduces the likelihood of compromised or malicious nodes being selected (or elected) as cluster 5heads.

Number of assumptions are made. Firstly, a reliable link layer protocol and cluster formation algorithm is assumed. [12]Once the clusters are formed they maintain the same members, except for cases where nodes are blacklisted die or when new nodes join the network.

All the nodes communicate via a shared bidirectional wireless channel and operate in the promiscuous mode, that is, if node A sends a message to node C via node B, then node A can hear if node B forwarded that message onto node C, the destination key distribution is not considered but it is assumed that each node has three keys; a master, cluster and pairwise. The master key is shared by every node and facilitate broadcast by the base station. Members of each cluster share the cluster key. Each cluster has a different cluster key. This key facilitates multicasting communication from the base station to a cluster and also group communication within the clusters themselves. The pairwise key allows node-to- node communication. [2]

Advantages:
1. This approach can decrease the likelihood of malicious or compromised nodes from becoming CHs.
2. It reduces the effect of bad mouthing attack.

Disadvantages:
1. TCHEM does not cover trust in detail because of which numerous key issues of trust management are not introduced.
2. Scalability of TCHEM model is not validated.

D. ATRM (Agent Based Trust and Reputation Management Scheme):

This technology introduces trust and reputation local management strategy with the aid of the mobile agents running on each node. The benefit of this local scheme is centralized repositories are not required for trust and reputation, and nodes themselves are capable of providing their own reputation information whenever required. [11]

The objective of the scheme is to manage trust and reputation locally with minimal overhead in terms of extra messages and time delay. This scheme shows extensive performance evaluation results, which clearly shows that trust and reputation can be computed in wireless sensor networks with minimal overhead. [8]

Advantages:
1. Centralized repositories are not required for trust and reputation.
2. Reputation computation and propagation is performed without network wide flooding and with no acquisition latency.
3. Minimum overhead is achieved in terms of extra messages and time delay.

Disadvantages:
1. The assumption, mobile agents are resilient against malicious nodes that try to steal or modify information that such agents carry may be unrealistic.
2. Very less attention to overhead on agents.

IV. Conclusion And Future Scope

This framework can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for co-operations between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Due to cancelling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes. The proposed secureprotocol can be used in most applications, not only one-to-one secure transmission, but also broadcasting and multi-casting. With the help of simulation results we can say that this model demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs. In future system can also save energy and increase the lifetime of a network. Also try to make more lightweight and reliable than the current system.

References

[1]. Fenye Bao, Ray Chen, MoonJeong Chang, and Jin-Hee Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management, 9(2):169–183, 2012.

[2]. Garth V Crosby, Niki Pissinou, and James Gadze. A framework for trust-based cluster head election in wireless sensor networks. In Second IEEE Workshop onDependability and Security in Sensor Networks and Systems, pages 10–pp. IEEE, 2006.

[3]. Saurabh Ganeriwal, Laura K Balzano, and Mani B Srivastava. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks(TOSN), 4(3):15, 2008.

[4]. Ablolfazl Afsharzadeh Kazerooni, Hamed Jelodar, and Javad Aramideh. Leach and heed clustering algorithms in wireless sensor networks: a qualitative study. Advances in Science and Technology Research Journal, 9(25), 2015.

[5]. Xiaoyong Li, Feng Zhou, and Junping Du. Ldts: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE transactions on information forensics and security, 8(6):924– 935, 2013.

[6]. Xiaoyong Li, Feng Zhou, and Xudong Yang. A multidimensional trust evaluation model for large-scale p2p computing. Journal of Parallel and Distributed Computing,71(6):837–847, 2011.

[7]. Zhengqiang Liang and Weisong Shi. Trecon: A trust-based economic framework for efficient internet routing. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(1):52–67, 2010.

[8]. Jaydip Sen. A survey on reputation and trust-based systems for wireless communication networks. arXiv preprint arXiv:1012.2529, 2010.

[9]. Riaz Ahmed Shaikh, Hassan Jameel, Brian J d'Auriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song. Group-based trust management scheme for clustered wireless sensor networks. IEEE transactions on parallel and distributed systems, 20(11):1698–1712, 2009.

[10]. Ivan Stojmenovic. Handbook of wireless networks and mobile computing, volume 27. John Wiley & Sons, 2003.

[11]. Yan Sun, Zhu Han, and KJ Ray Liu. Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 46(2):112–119, 2008.

[12]. Yan Lindsay Sun, Wei Yu, Zhu Han, and KJ Ray Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, 24(2):305–317, 2006.

[13]. Dali Wei, Yichao Jin, Serdar Vural, Klaus Moessner, and Rahim Tafazolli. An energy-efficient clustering solution for wireless sensor networks. IEEE transactions on wireless communications, 10(11):3973–3983, 2011.

[14]. Guoxing Zhan,Weisong Shi, and Julia Deng. Tarf: A trustaware routing framework for wireless sensor networks. In European Conference onWireless Sensor Networks, pages 65–80. Springer, 2010.