© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Trust Based Mechanism in Wireless Sensor Network

Pratishtha Gupta*, Prof. Nitin Tiwari
Computer Science and Engineering Department, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

WSNs are important to enemies and they get to be powerless to a few sorts of assaults since they are sent in open and unprotected situations. Because of the constrained assets of WSNs, it is trying to consolidate essential security components, for example, verification, key conveyance and protection in WSNs. In any case, trust administration that models the trust on the conduct of components of the system, can be particularly helpful for a sensor system environment to improve security. Trust administration plots that are focused at sensor systems should be lightweight regarding computational and correspondence prerequisites, yet effective as far as adaptability in overseeing trust between hubs of heterogeneous sending. This paper reviews different trust administration plans proposed for remote sensor system.

Keywords: Wireless sensor networks (WSN); Security; Quality of Service (QoS); Stochastic Petri Net (SPN) ; Trust management

I. INTRODUCTION

A remote sensor system comprises of spatially dispersed self-sufficient sensors to screen and respond to ecological conditions and send the gathered information to a war room utilizing remote channels. The equipment parts of a sensor hub incorporate a radio handset, an inserted processor, inside and outer recollections, a force source and one or more sensors [1]. A sensor hub can sense and forward the data through multi jump steering. The essential security objectives for sensor systems are secrecy, uprightness, accessibility and verification of information [2]. It is conceivable that the developing significance of sensor systems could be impeded by their inborn security issues. It is then basic to give an arrangement of security primitives and administrations that can ensure those systems and enhance their strength and dependability.

Because of constrained assets of WSNs, it is trying to consolidate essential security capacities, for example, confirmation and protection. Thus, remote sensor systems are inclined to various sorts of noxious assaults, for example, refusal of administration, directing convention assaults and so forth. Conventional crypto plans are unequipped for averting such for a sensor network environment. However traditional trust management schemes developed for wired and wireless networks may not be suitable for networks with small sensor nodes due to limited bandwidth and memory constraints. Trust management can help improving the security of WSN. For example, for the routing process, sensor nodes might need to know which other nodes to trust for forwarding a packet. For sensing purposes a node might need to trust other neighbouring nodes for checking anomalous measurements [3]. However, as sensor nodes are usually constrained devices, the trust management systems must be lightweight enough to provide a good performance without hindering the functionality of the system. This survey deals with various trust management schemes proposed for WSNs.

II. METHODS AND MATERIAL

Literature Survey

Researchers are developed various trust management schemes for WSNs. Some of the innovative approaches are described here.

A. Trust Management for Resilient Geographic Routing (TM-RGR) [4]

The creators propose a calculation for area check and trust model for maintaining a strategic distance from assaults on geographic steering. The fundamental thought here is to support well carrying on legit hubs by giving them the kudos for each effective bundle sending while punishing suspicious hubs that as far as anyone knows lie about or overstate their commitment to directing. In the event that a hub lies about its area, it is quickly rejected from the sending set. Fair hub with great correspondence connection to the destination will stay longer time in the sending set. After a hub develops a steering table, it screens the conduct of its one jump neighbors to which it advances the parcels by utilizing snooping or catching methods.

It is an extremely basic trust model. The figuring of trust redesign esteem takes less time. Be that as it may, the exactness is less and the shot of false positives and false negatives are high.

B. Hybrid Trust and Reputation Management (HTRM) [5]

This paper proposes a hybrid trust management model that combines aspects from behavior based and certificate based approaches. Certificates marked by the online trust administration powers and conduct based trust are utilized for trust figuring. Trust of a hub is assessed in the wake of amassing enough number of confirmations from testament power or exceptionally trusted hubs or from neighbors. Suggestions from most elevated referral hubs are gathered if endorsement power's authentication is not suffice. At the point when negative proofs are gathered, an authentication or trust can be renounced. Trust relationship between trust guarantor i and trust target j depend on the accompanying blends: (a) privately put away data of i on the part based trust affiliations that were set up preceding sending, (b) legitimate authentications that j can give to i, (c) suggestions got for j upon solicitation by outsiders that i has a trust relationship with, and (d) conduct based trust assessment by supervision hubs that i has a trust relationship with. The initial two are the verifiable suggestions from the system proprietor and trust overseeing powers and the last two are express ones.

The paper considers both immediate and roundabout perceptions to compute the trust. In any case, high computational force is required for assessing both behavioral and authentication acceptance**.**

C. Group Based Trust Management Scheme (GBTMS) [6]

In this paper, trust is assessed for a gathering of sensor hubs rather than single sensor hub. The creators propose a light weight calculation which utilizes grouping. GBTMS deals with two topologies: (1) intergroup topology where dispersed trust administration methodology is utilized and (2) intergroup topology where brought together trust administration methodology is utilized. It gives some level of counteractive action component notwithstanding recognizing malignant hubs.

GBTMS computes the trust values in view of immediate and roundabout perceptions. Direct perceptions speak to the quantity of fruitful and unsuccessful connections in the middle of hubs and aberrant perceptions speak to the proposals of trusted companions around a particular hub. Every group head assesses other bunch heads and sensor hubs under its bunch.

The primary favourable position of this strategy is that memory utilization is less since it utilizes unsigned whole number trust esteem and trust of a gathering of hubs are assessed. Yet, the measure of assets and force required are more since it depends on show based procedure furthermore the trust is computed in view of the past collaboration encounters in message conveyance. A hub may manufacture notoriety and begin acting noxiously. In any case, this paper accepts that a decent hub is constantly genuine.

D. Trust Management Architecture (TMA) [7]

A novel hierarchical trust management scheme that minimizes communication and storage overheads is proposed by the authors. This scheme considers both direct and indirect trust in trust evaluation. This paper introduces a new node called a sponsor node in the network. Sponsor node selects the target nodes based on both trust and energy of the target nodes. The main focus of this paper will be to develop a formal model for modelling trust in hierarchical ad hoc sensor networks to enable mobile sensor nodes to form, maintain, and exchange trust opinions with minimal overheads in terms of complex computations at sensor nodes. Node's memory consumption is minimized by storing the trust information at the cluster head. This method has the ability to consider the movement of nodes from one cluster to another. But the memory and computation overhead of cluster heads are more.

E. Weighted Trust Evaluation (WTE) [8]

In this paper, the authors proposed a weighted trust evaluation (WTE) based scheme to detect the compromised nodes by monitoring its reported data. It is a light-weighted algorithm that would incur little overhead. Considering the scalability and flexibility, hierarchical network architecture is adopted in the paper. Sensor nodes in sensor networks are usually deployed in hostile environments such as battle fields. Consequently a sensor node may be compromised or out of function and then provides wrong information that may mislead the whole network. It is therefore an important issue to detect the malicious nodes in the sensor network.

Updating the weight of each sensor node has two purposes. First, if a sensor node is compromised and frequently sends its report inconsistent with the final decision its weight is likely to be decreased. Then if a sensor node’s weight is lower than a specific threshold, identify it as a malicious node. Second, the weight also decides how much a report may contribute to the final decision. This is reasonable since if the report from a sensor node tends to be incorrect, it should be counted less in the final decision. Even though the weight value is updated dynamically, the chance of false probability is more.

F. Weighted Trust Algorithm (WTA) [9]

The authors propose a scheme for malicious node detection based on weighted trust evaluation which is an improvement of WTE algorithm [8]. The authors apply the weighted trust detection scheme to military surveillance and reconnaissance applications and which makes the update of node's weight value more accurate and misdetection ratio lower significantly.

A weight value is assigned to each sensor node initially. It updates every cycle if the node sends different report from the other sensor nodes. A malicious node is detected when its weight value is lower than a threshold value. A node's weight is higher means the node is more trustful. In this paper the weight value is updated dynamically. The main drawbacks are chance of false positive probability is more and also forwarding node may fail leading to problems.

G. Behaviour Trust based on Geometric Mean Approach (BTGMA) [10]

This paper proposes another trust administration framework by considering the practices of sensor hubs. Both immediate and circuitous trusts in light of geometric mean of the nature of administration attributes among the hubs are considered for trust estimation which permits the trusted hubs just to take an interest in message directing. The nature of administration qualities considered are bundle forward, information rate, power utilization, unwavering quality and so on. Directing of information can happen through the ordinary or altruistic hubs present in the system and along these lines it decreasing bundle inactivity and dropping of parcels.

Geometric mean based trust administration framework is a trust model suitable for some viable uses of the WSNs. This model is a decentralized trust plan implies the trust administration usefulness is disseminated over the system hubs. Every hub is in charge of figuring its own particular trust esteem per connection in the system, gathering occasions from direct relations, and gathering trust values from different hubs in the system. This aberrant data might be helpful when no or restricted direct collaboration has been experienced.

The principle favorable position of BTGMA is that the base edge quality can be given to every trust metric we are considering while most different strategies considers just general edge esteem for the whole trust metric. So this strategy is more precise however the overhead is more.

H. Hierarchical Trust Management (HTM) [11]

The creators propose a progressive trust administration convention for WSNs to manage childish and malevolent hubs. This paper considers both QoS trust and social trust to judge if a hub is trust commendable. A novel likelihood model called stochastic Petri net is utilized to portray the arranged WSN to discover the ground truth character. Various levelled trust administration convention can powerfully gain from past encounters and adjust to changing natural conditions to expand the application execution. This is accomplished by tending to basic issues of various leveled trust administration to be specific trust creation, collection, and development. Trust arrangement considers what trust segments are utilized, trust accumulation considers how data is totaled for every trust segment and trust development considers how trust is shaped from individual trust parts. The target trust got from worldwide learning or ground truth got from SPN model can be analyzed and accepted against the subjective trust got as consequence of executing the trust administration convention.

At sensor hub level, every sensor hub assesses other sensor hubs in the same group and sends the outcome to bunch head. At bunch head level, every group head assesses every sensor hub in same group and other bunch heads and sends the outcome to group head officer. The convention considers two nature of administration trust segments specifically vitality and unselfishness and two social trust parts in particular closeness and trustworthiness for trust figuring.

The convention presents another configuration idea of utilization level trust streamlining because of changing ecological conditions to boost application execution or best fulfill application prerequisites. This trust administration convention can apply to any WSN comprising of heterogeneous sensor hubs with boundlessly distinctive starting vitality levels and diverse degrees of malevolent or egotistical practices. To show the utility of progressive trust administration convention, the creators apply it to trust based geographic steering and trust based interruption identification. This technique is more exact however the disappointment of bunch head may prompt issues.

I. Lightweight and Dependable Trust management Scheme (LDTS) [12]

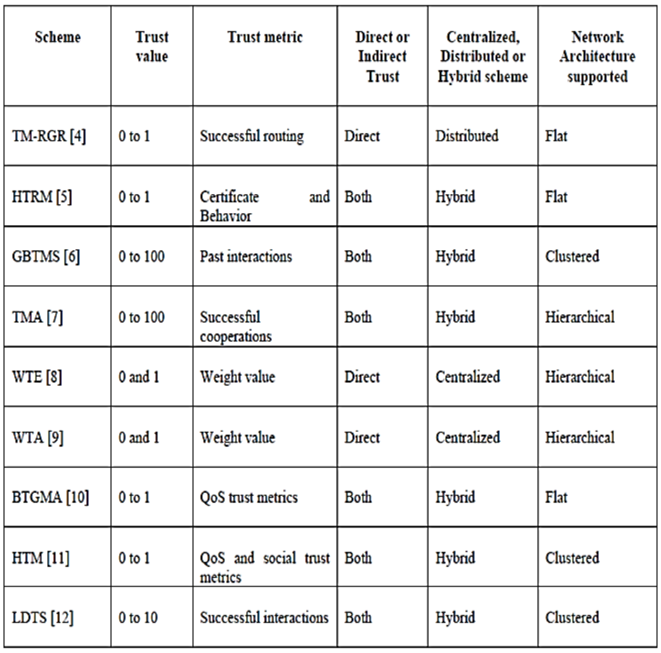
LDTS facilitates trust decision making based on a light weight scheme. By closely considering the identities of nodes in clustered WSNs, this scheme reduces risk and improves system efficiency while solving the trust evaluation problem when direct evidence is insufficient. Most trust management systems proposed for WSNs adopt simple weighted average approaches to aggregate feedback trust information without considering the issue of malevolent criticism. This may prompt misjudgment of the trust basic leadership process. Be that as it may, LDTS does not use show based technique and rather sets the estimation of backhanded trust in light of the criticism reported by the bunch head around a hub. This criticism component has various favorable circumstances, for example, the viable moderation of the compelling malignant input, in this manner diminishing the systems administration hazard in an open or threatening WSN environment. Since the criticism between bunch individuals need not be viewed as this component can altogether diminish system correspondence overhead therefore enhancing the framework asset proficiency. The principle commitments of the LDTS paper are: (an) a light weight trust assessment plan for participation between bunch individuals or group heads; (b) a reliability improved trust assessing approach for collaboration between group heads; and (c) a self-versatile weighting technique for group head's trust accumulation. The overhead of this methodology is less and it is a tried and true trust administration framework. In any case, if the bunch head is fizzled or bargained, then this methodology won't work. On the off chance that a vindictive client begins foreswearing of administration assault then the bunch head would be squandering its time in answering to pernicious clients thus denying great clients from utilizing the administration of group head.

III. RESULTS AND DISCUSSION

Analysis

Different parameters are identified for comparing the trust management schemes discussed. The parameters are trust value, trust metric, direct or indirect trust, centralized, distributed or hybrid scheme, and the network architecture supported by the trust management scheme. Table 1 shows the comparison of different trust schemes discussed. [4], [5], [10] and [11] consider trust values as real values from 0 to 1 and [8], [9] consider only 0 (distrust) and 1 (complete trust) as trust values. [6] and [7] consider trust values as unsigned integers from 0 to 100. [12] Consider trust value as unsigned integer from 0 to10. An unsigned integer from 0 and 10 only needs 4 bits of memory space and between 0 and 100 needs 1 byte of memory. The real value representation of trust value requires 4 bytes of memory space. The trust metric considered for trust calculation, type and the architecture supported by the trust scheme are shown in the Table 1. Except [4], [8] and [9], all other schemes use both direct observation and indirect recommendation for trust calculation.

Table 1. Comparison of trust schemes



Scheme	Trust value	Trust metric	Direct or Indirect Trust	Centralized, Distributed or Hybrid scheme	Network Architecture supported
TM-RGR [4]	0 to 1	Successful routing	Direct	Distributed	Flat
HTRM [5]	0 to 1	Certificate and Behavior	Both	Hybrid	Flat
GBTMS [6]	0 to 100	Past interactions	Both	Hybrid	Clustered
TMA [7]	0 to 100	Successful cooperations	Both	Hybrid	Hierarchical
WTE [8]	0 and 1	Weight value	Direct	Centralized	Hierarchical
WTA [9]	0 and 1	Weight value	Direct	Centralized	Hierarchical
BTGMA [10]	0 to 1	QoS trust metrics	Both	Hybrid	Flat
HTM [11]	0 to 1	QoS and social trust metrics	Both	Hybrid	Clustered
LDTS [12]	0 to 10	Successful interactions	Both	Hybrid	Clustered

IV. CONCLUSION

The trust framework takes a shot at the suspicion that a lion's shares of hubs in an area are dependable. This overview manages different trust administration plans for WSNs. Some trust administration frameworks use both immediate and backhanded perceptions to compute the trust quality and others utilize just direct perception to figure the trust. The trust framework is more dependable when both immediate and circuitous perceptions are considered. All trust administration frameworks proposed for WSNs consider just certain QoS trust parameters for ascertaining the trust esteem. Since the HTM [11] paper proposed by Fenye Bao et al. considers both QoS and social trust parameters for ascertaining the trust, the trust worth is more exact.

V. REFERENCES

[1] Qinghua Wang and Ilangko Balasingham, "Wireless sensor networks - an introduction".

[2] G. Padmavathi and D.Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," volume 4, pages 1 - 9, International Journal of Computer Science and Information Security, 2009.

[3] Sakshi Srivastava and Kushal Johari, “A survey on reputation and trust management in wireless sensor network," volume 1, pages 139 -149, International Journal of Scientific Research Engineering Technology, August 2012.

[4] Ke Liu, Nael Abughazaleh and Kyoung Donkang., "Location verification and trust management for resilient geographic routing," ELSEVIER, 2007

[5] Efthimia Aivaloglou and Stefanos Gritzalis, "Hybrid trust and reputation management for sensor networks," Springer, October 2009.

[6] 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," pages 1698 - 1712, IEEE Transactions on Parallel and Distributed Systems, October 2009.