A Survey on Trust Management in Wireless Sensor Networks

Reshmi . V
M.tech Student
Computer Science & Engineering
M.E.S. College of Engineering
Kuttippuram, Kerala
reshmi.nalinam@gmail.com

Sajitha . M
Asst. Professor
Computer Science & Engineering
M.E.S. College of Engineering
Kuttippuram, Kerala
sajitha139@gmail.com

Abstract - Wireless Sensor Network consists of spatially distributed autonomous sensors to monitor environmental or physical conditions and has many practical applications. WSNs are of interest to adversaries and they become susceptible to some types of attacks since they are deployed in open and unprotected environments. Due to the limited resources of WSNs, it is challenging to incorporate basic security features such as authentication, key distribution and privacy in WSNs. But, trust management that models the trust on the behavior of elements of the network, can be especially useful for a sensor network environment to enhance security. Trust management schemes that are targeted at sensor networks need to be lightweight in terms of computational and communication requirements, yet powerful in terms of flexibility in managing trust between nodes of heterogeneous deployment. This paper surveys various trust management schemes proposed for wireless sensor network.

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

I. INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to monitor and react to environmental conditions and send the collected data to a command center using wireless channels. The hardware components of a sensor node include a radio transceiver, an embedded processor, internal and external memories, a power source and one or more sensors [1]. A sensor node can sense and forward the information through multi hop routing. The primary security goals for sensor networks are confidentiality, integrity, availability and authentication of data [2]. It is possible that the emerging importance of sensor networks could be hindered by their inherent security problems. It is then imperative to provide a set of security primitives and services that can protect those networks and improve their robustness and reliability.

Due to limited resources of WSNs, it is challenging to incorporate basic security functions such as authentication and privacy. As a result, wireless sensor networks are prone to different types of malicious attacks, such as denial of service, routing protocol attacks etc. Traditional crypto schemes are incapable of preventing such types of malicious attacks. Trust management, which models the trust on the behavior of the elements of the network, can be especially useful 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 neighboring 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. 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 authors propose an algorithm for location verification and trust model for avoiding attacks on geographic routing. The basic idea here is to favor well behaving honest nodes by giving them the credit for each successful packet forwarding while penalizing suspicious nodes that supposedly lie about or exaggerate their contribution to routing. If a node lies about its location, it is immediately excluded from the forwarding set. Honest node with good communication link to the destination will remain longer time in the forwarding set. After a node constructs a routing table, it monitors the behavior of its one hop neighbors to which it forwards the packets by using snooping or overhearing techniques.

It is a very simple trust model. The calculation of trust update value takes less time. But the accuracy is less and the chance 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 signed by the online trust management authorities and behavior based trust are used for trust calculation. Trust of a node is evaluated after accumulating enough number of evidences from certificate authority or highly trusted nodes or from neighbors. Recommendations from highest referral nodes are collected if certificate authority's certificate is not suffice. When negative evidences are collected, a certificate or trust can be revoked.

Trust association between trust issuer i and trust target j are based on the following combinations: (a) locally stored information of i on the role based trust associations that were established prior to deployment, (b) valid certificates that j can provide to i, (c) recommendations received for j upon request by third parties that i has a trust association with, and (d) behavior based trust evaluation by supervision nodes that i has a trust association with. The first two are the implicit recommendations from the network owner and trust managing authorities and the latter two are explicit ones.

The paper considers both direct and indirect observations to calculate the trust. But high computational power is needed for evaluating both behavioral and certificate validation.

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

In this paper, trust is evaluated for a group of sensor nodes instead of single sensor node. The authors propose a light weight algorithm which employs clustering. GBTMS works on two topologies : (1) intragroup topology where distributed trust management approach is used and (2) intergroup topology where centralized trust management approach is used. It provides some degree of prevention mechanism in addition to detecting malicious nodes.

GBTMS calculates the trust values based on direct and indirect observations. Direct observations represent the number of successful and unsuccessful interactions between nodes and indirect observations represent the recommendations of trusted peers about a specific node. Each cluster head evaluates other cluster heads and sensor nodes under its cluster.

The main advantage of this method is that memory consumption is less since it uses unsigned integer trust value and trust of a group of nodes are evaluated. But the amount of resources and power needed are more since it relies on broadcast based strategy and also the trust is calculated based on the past interaction experiences in message delivery. A node may build reputation and start behaving maliciously. But this paper assumes that a good node is always honest.

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 modeling 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. Behavior Trust based on Geometric Mean Approach (BTGMA) [10]

This paper proposes a new trust management system by considering the behaviors of sensor nodes. Both direct and indirect trusts based on geometric mean of the quality of service characteristics among the nodes are considered for trust calculation which allows the trusted nodes only to participate in message routing. The quality of service characteristics considered are packet forward, data rate, power consumption, reliability etc. Routing of data can takes place through the normal or benevolent nodes present in the network and thus it reducing packet latency and dropping of packets.

Geometric mean based trust management system is a trust model suitable for many practical applications of the WSNs. This model is a decentralized trust scheme means the trust management functionality is distributed over the network nodes. Each node is responsible for computing its own trust value per relation in the network, collecting events from direct relations, and collecting trust values from other nodes in the network. This indirect information may be useful when no or limited direct interaction has been experienced.

The main advantage of BTGMA is that the minimum threshold value can be given to each trust metric we are considering while most other methods considers only an overall threshold value for the entire trust metric. So this method is more accurate but the overhead is more.

H. Hierarchical Trust Management (HTM) [11]

The authors propose a hierarchical trust management protocol for WSNs to deal with selfish and malicious nodes. This paper considers both QoS trust and social trust to judge if a node is trust worthy. A novel probability model called stochastic petri net is used to characterize the assorted WSN to find the ground truth character.

Hierarchical trust management protocol can dynamically learn from past experiences and adapt to changing environmental conditions to maximize the application performance. This is achieved by addressing critical issues of hierarchical trust management namely trust composition, aggregation, and formation. Trust composition considers what trust components are used, trust aggregation considers how information is aggregated for each trust component and trust formation considers how trust is formed from individual trust components. The objective trust derived from global knowledge or ground truth derived from SPN model can be compared and validated against the subjective trust obtained as result of executing the trust management protocol.

At sensor node level, each sensor node evaluates other sensor nodes in the same cluster and sends the result to cluster head. At cluster head level, each cluster head evaluates each sensor node in same cluster and other cluster heads and sends the result to cluster head commander. The protocol considers two quality of service trust components namely energy and unselfishness and two social trust components namely intimacy and honesty for trust calculation.

The protocol introduces a new design concept of application level trust optimization in response to changing environmental conditions to maximize application performance or best satisfy application requirements. This trust management protocol can apply to any WSN consisting of heterogeneous sensor nodes with vastly different initial energy levels and different degrees of malicious or selfish behaviors. To demonstrate the utility of hierarchical trust management protocol, the authors apply it to trust based geographic routing and trust based intrusion detection. This method is more accurate but the failure of cluster head may lead to problems.

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 problem of malicious feedback. This may lead to misjudgment of the trust decision making process. But LDTS does not utilize broadcast based strategy and instead sets the value of indirect trust based on the feedback reported by the cluster head about a node. This feedback mechanism has numerous advantages such as the effective mitigation of the effective malicious feedback, thereby reducing the networking risk in an open or hostile WSN environment. Because the feedback between cluster members need not be considered this mechanism can significantly reduce network communication overhead thus improving the system resource efficiency.

The main contributions of the LDTS paper are : (a) a light weight trust evaluation scheme for cooperation between cluster members or cluster heads; (b) a dependability enhanced trust evaluating approach for cooperation between cluster heads ; and (c) a self adaptive weighting method for cluster head's trust aggregation. The overhead of this approach is less and it is a dependable trust management system. But if the cluster head is failed or compromised, then this approach will not work. If a malicious user starts denial of service attack then the cluster head would be wasting its time in replying to malicious users hence denying good users from using the service of cluster head.

III. 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 system works on the assumption that a majority of nodes in a neighborhood are reliable. This survey deals with various trust management schemes for WSNs. Some trust management systems use both direct and indirect observations to calculate the trust value and others use only direct observation to calculate the trust. The trust system is more reliable when both direct and indirect observations are considered. Almost all trust management systems proposed for WSNs consider only certain QoS trust parameters for calculating the trust value. Since the HTM [11] paper proposed by Fenye Bao et al. considers both QoS and social trust parameters for calculating the trust, the trust value is more accurate.

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.

[7] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan, and Abdul Sattar, "A trust management architecture for hierarchical wireless sensor networks," pages 268 - 271, IEEE Conference, 2010.
[8] Idris M. Atakli, Hongbing Hu, Yu Chen, WeiShinn Ku, and Zhou Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation, " The Symposium on Simulation of Systems Security (SSSS08), Ottawa, Canada,, April 2008.
[9] Long Ju, Hongjuan Li, Yaqiong Liu, Weilian Xue, Keqiu Li, and Zhongxian Chi," An improved intrusion detection scheme based on weighted trust evaluation for wireless sensor networks", IEEE Conference on Local Computer Networks, 2010.
[10] Satya Keerthi, A Manogna, Yasaswini, A Aparna, and Ravi Teja, "Behaviour based trust management using geometric mean approach for wireless sensor networks," volume 3, pages 229 - 234, International Journal of Computer Trends and Technology, 2012.
[11] Fenye Bao, Ing-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," volume 9, pages 169 - 183, IEEE transactions on network and service management, June 2012.
[12] Xiaoyong Li, Feng Zhou, and Junping Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," volume 8, pages 924-935, IEEE Transactions on Information Forensics and Security, June 2013.