www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 03 Issue 07 July, 2014 Page No. 6982-6984

A Reactive Hierarchical Trust Management Scheme for Wireless Sensor Networks

Reshmi V[1], Sajitha M[2]

[1]M.Tech Student, Computer Science Department,
MES college of Engineering, Kuttippuram, Kerala, India
reshmi.nalinam@gmail.com

[2]Assistant Professor, Computer Science Department,
MES college of Engineering, Kuttippuram, Kerala, India
sajitha139@gmail.com

Abstract: Wireless sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure etc. and cooperatively pass their data through the network to a main location. However, individual sensor nodes are vulnerable to some types of attacks because they are usually deployed in open and unprotected environments. Trust management, which models the trust on the behavior of the elements of the network, can be especially useful for a sensor network environment to enhance security. Various methods have been proposed for trust management in wireless sensor networks. A reactive hierarchical trust management scheme is proposed here which reduces the energy consumption rate of sensor nodes by calculating the trust values on demand.

Keywords: Wireless sensor networks (WSN), Security, Trust management.

1. Introduction

A wireless sensor network (WSN) 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 multihop routing. It is possible that the emerging importance of sensor networks could be hindered by their inherent security problems.

The main characteristics of WSNs are:

(1) Communication paradigm : Compared to traditional communication networks, individual node Identifiers (IDs) are not important. Instead, WSNs are data-centric meaning that the communication should be targeted to nodes in a given location or with a defined data content.
(2) Application specific : WSN is deployed to perform a specific task.
(3) Dynamic nature : In a typical WSNs, node platforms are error-prone due to harsh operating conditions. Communication links between nodes are not stable due to node errors, unreliable and simple modulations, mobility of nodes, and environmental interferences.
(4) Scale and density : Compared to other wireless networks, the number of nodes comprising WSNs may be huge. Further, the density of nodes can be high.
(5) Resource constraints : A typical WSN node is small in physical size and battery powered. This implies that computation, communication, and memory resources in nodes are very limited.
(6) Deployment : In large-scale WSNs, the deployment of nodes is random and their maintenance and replacement is impractical. Still, the requirements and applications of the deployed WSN may alter, which implicate that runtime reconfiguration and reprogramming are needed.

The main requirements of WSNs are:

(1) Fault tolerance : The network functionality must be maintained even though the built-in dynamic nature and failures of nodes due to harsh environment, depletion of batteries, or external interference make networks prone to errors.
(2) Lifetime : The nodes are battery powered or the energy is scavenged from the environment and their maintenance is difficult. Thus, energy saving and load balancing must be taken into account in the design and implementation of WSN platforms, protocols, and applications.
(3) Scalability : The number of nodes in WSN is typically high. Thus, the WSN protocols must deal with high densities and numbers of nodes.
(4) Real time : WSNs are tightly related to the real world. Therefore, strict timing constraints for sensing, processing, and communication are present in WSNs.
(5) Security : The need for security in WSNs is evident, especially in health care, security, and military applications.

Most of the applications relay data that contain private or confidential information.

(6) Production cost : The number of nodes in WSNs is high, and once nodes run out of batteries they are replaced by new ones. Further, WSNs are envisioned to be everywhere. Therefore, to make the deployments possible, the nodes should be extremely low cost.

Due to limited resources of WSNs, it is challenging to incorporate basic security functions such as authentication and privacy in WSNs. As a result, wireless sensor networks are prone to different types of malicious attacks, such as denial of service, routing protocol attacks etc. Trust management can help improving the security of WSN.

2. Literature Survey

Researchers are developed various trust management schemes for wireless sensor networks. Some of the innovative approaches to trust management in wireless sensor networks are described here.

Ke Liu et al. [2] proposes an algorithm for location verification and trust model for avoiding attacks on geographic routing. The basic idea here is to favour 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. Even though it is a simple trust model, the chance of false positives and false negatives are high.

Efthimia Aivalogue et al. [3] proposes a hybrid trust management model that combines aspects from behaviour based and certificate based approaches. Trust of a node is evaluated after accumulating enough number of evidences from certificate authority or highly trusted nodes or from neighbours. 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. Any type of network is supported by hybrid trust model. But high computational power is needed for evaluating both behavioural and certificate validation.

Idris M. Atakli et al. [4] develop a scheme for malicious node detection based on weighted trust evaluation (WTE). A malicious node will be detected when its weight value is lower than a threshold value. Weight value is updated dynamically. If the forwarding node fails then it may leads to problems.

Behavior based trust management scheme proposed by Ch. Satyakeerthi N.V.L. et al. [5] consider the quality of service characteristics such as packet forward, data rate etc. for trust calculation. This is a decentralized trust scheme. Since this paper does not consider any social characteristics of the network for trust evaluation, the trust values are not believable.

Fenye Bao et al. [6] proposes a hierarchical trust management protocol for wireless sensor networks 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 [7] is used to characterize the assorted WSN to find the ground truth character. At sensor node level, each sensor node evaluates other sensor nodes in 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. 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.

3. Reactive Hierarchal Trust Management Scheme (RHTM)

In the proposed work, reactive hierarchical trust management scheme for wireless sensor network (RHTM), the network is divided into a number of clusters. Cluster heads are selected prior to deployment. Trust values are calculated on demand.

3.1 Trust management in RHTM

Each cluster head evaluates the sensor nodes in its cluster based on the report from the neighbouring sensor nodes and the base station evaluates each cluster head based on the report from the neighbouring cluster heads. Trust value is calculated based on the two QoS trust metrics energy and unselfishness and two social trust metrics intimacy and honesty. In RHTM, the trust values of sensor nodes are calculated only reactively upon the request from the cluster head and the trust values of cluster heads are calculated reactively upon the request from the base station. The trust values are calculated same as the paper hierarchical trust management (HTM) [6].

4. Implementation Results

4.1 Simulation Parameters

The project is implemented using NS2. Nodes are static and all nodes have equal energy initially. Cluster heads are predetermined. After the formation of hierarchical architecture, trust values are calculated based on energy, unselfishness, intimacy and honesty.

The network simulation parameters are shown in table 1. Number of nodes considered are 100 in an area of 1000 meter^2.The 100 nodes form 5 clusters and the number of access point is one. All nodes have equal energy initially and nodes are static.

Table 1: Simulation parameters

Parameter	Value
Number of nodes	100
Network area	1000 meter^2
Number of clusters	5
Number of access points	1
Simulation time	100 seconds
Node movement	None
Traffic type	CBR

4.2 Results

Trust management helps to improve the security of wireless sensor networks. The trust value helps to detect if a node is malicious or not. The reactive hierarchical trust management scheme has been compared with hierarchical trust management scheme based on the energy consumption rate.

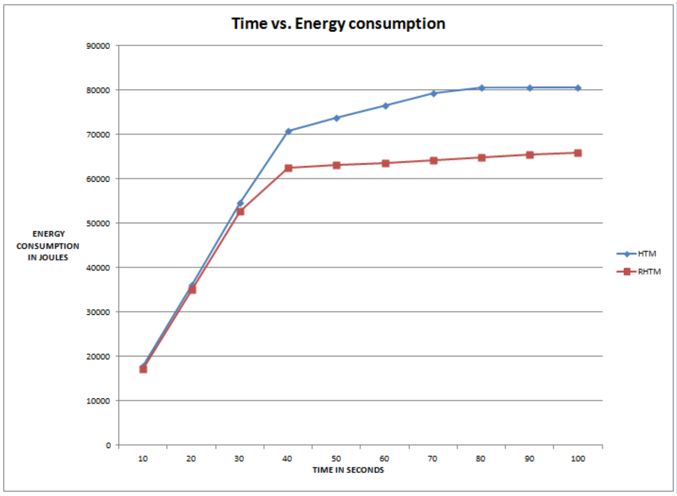

Figure 1: Energy consumption rate

Energy consumption rate of reactive hierarchical trust management (RHTM) versus hierarchical trust management (HTM) is shown in fig. 1. From the figure, it is clear that the energy consumption rate of RHTM is less than that of HTM since trust values are calculated reactively in RHTM.

5. Conclusion

The Wireless Sensor Network is an emerging research area which has wide range of applications. Hence the security in wireless sensor network is very important. Trust management helps to improve the security of wireless sensor networks. Various methods have been developed for trust management in wireless sensor networks. Reactive hierarchical trust management scheme is an enhanced method for trust management which reduces the energy consumption rate of trust management.

There are some future research directions in this field. There may be some attackers in the network who will give wrong recommendations but will forward the packets correctly. Reactive hierarchical trust management scheme cannot identify those types of attacks. Such types of active attackers can be eliminated by introducing some new mechanism.

References

[1] Qinghua Wang and Ilangko Balasingham, ”Wireless Sensor Networks - An Introduction”, InTech Publisher, December, 2010.

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

[3] Efthimia Aivaloglou, and Stefanos Gritzalis, ”Hybrid trust and reputation management for sensor networks”, *Springer*, October, 2009.

[4] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn 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 14 - 17, 2008.

[5] Ch. Satya Keerthy. N.V.L, A. Manogna, Ch. Yasaswini, A. Aparna and S.Ravi Teja, ”Behaviour based Trust Management using geometric mean approach for Wireless Sensor Networks”, *International Journal of Computer Trends and Technology*, pp. 229-234, vol. 31, no. 2, 2012.

[6] 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”, *IEEE Transactions on Network and Service Management*, pp. 169-183, vol. 9, no. 2, June 2012.

[7] R. A. Sahner, K. Trivedi, and A. Puliafito, "Performance and Reliability Analysis of Computer Systems", *Kluwer Academic Publishers*, 1996.