It is the paper published as:

Author: T. Zia
Title: Reputation-based Trust Management in Wireless Sensor Networks
Editor: S. Bouzerdoum
Conference Name: Fourth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2008
Conference Location: Sydney, NSW Australia
Publisher: IEEE Xplore
Year: 2008
Pages: 163-166
Date: December 15-18, 2008

Abstract: Wireless sensor networks are promising future of many sensitive applications such as healthcare, defence, habitat monitoring and early bushfire detection. These networks are prone to security attacks due to their wireless and deployment nature. It is very likely that after deployment of the network, sensor nodes are left unattended which causes serious security concerns. Insecure wireless communication aggravates the inherent vulnerabilities of wireless sensor networks. This paper is to study the reputation and trust management and setting a scene to integrate the trust in a security framework to ensure the reliability, integrity and trustworthiness of data sensed by the sensor nodes.

Author Address: tzia@csu.edu.au

URL: http://dx.doi.org/10.1109/ISSNIP.2008.4761980

http://www.elec.uow.edu.au/issnip2008/index.html

Reputation-based Trust Management in Wireless Sensor Networks

Tanveer Zia
School of Computing & Mathematics
Charles Sturt University, NSW 2678
tzia@csu.edu.au

Abstract

Wireless sensor networks are promising future of many sensitive applications such as healthcare, defence, habitat monitoring and early bushfire detection. These networks are prone to security attacks due to their wireless and deployment nature. It is very likely that after deployment of the network, sensor nodes are left unattended which causes serious security concerns. Insecure wireless communication aggravates the inherent vulnerabilities of wireless sensor networks. This paper is to study the reputation and trust management and setting a scene to integrate the trust in a security framework to ensure the reliability, integrity and trustworthiness of data sensed by the sensor nodes.
.

1. INTRODUCTION

The aim of this paper is to investigate reputation and trust management schemes in mobile ad hoc and sensor networks and set the ground work to integrate it in a security framework to avoid computationally expensive cryptographic techniques to preserve the computational resources and energy of wireless sensor networks. The significance of the paper is due to the potential of sensor networks to be deployed in mission critical and sensitive applications in defence, healthcare, habitat and bush fire monitoring, and several other commercial applications. Due to the wireless and unattended deployment nature of sensor networks, there is a risk of unique threats, along with the aim to ensure the confidentiality, integrity and reliability of communication over these networks. Although considerable developments have been made towards counteracting potential threats in sensor networks, these security measures remain inadequate. Most of the solutions available in literature address a specific security problem but ignore others; those which achieve low energy and memory consumption compromise on the level of security. None of these solutions is able to simultaneously ensure low energy and memory consumption and provide complete security. Thus there is a need for a better security system which can combine low operational costs with a high security performance. This paper investigates reputation and trust management schemes with an intention to integrate it in our security framework [1] to provide a comprehensive security solution against the known threats thus far encountered in sensor networks. The concept of establishing reputation and trust among sensor nodes in a security framework seems to be a desirable solution where nodes monitor their neighbouring nodes and rank the neighbours in terms of a trust vote. The higher the vote the better is the trust value. Rest of the paper is organised as below:

Section 2 provides a summary of related work in trust management in ad hoc and wireless sensor networks. Section 3 and 4, discuss the threat and trust model respectively addressed in the proposed scheme. In section 5, a preliminary proposal of a reputation-based trust management scheme is presented with some analysis illustrated in figures. In section 6, an experimental evaluation of the proposed scheme is provided followed by conclusion and future work in section 7.

2. RELATED WORK

Bourke and Li [2] proposed an agent based trust and reputation management scheme from system design perspectives. They have used a localised trust model and reputation management strategy to reduce the communication cost and acquisition latency. In this scheme an agent launcher is assumed a trusted authority for generating and launching a mobile agent called *trust and reputation assessor* designed to be distributed in every node and provide hosting node the trust and reputation management service. Ren et al. [3] have addressed the trust management in terms of social relationship among nodes by proposing a certificate-based scheme which requires a boot strapping phase during which a secret dealer is required. After boot strapping network becomes functional without need of the dealer. A security framework with trust management for sensor networks is proposed by Yao et al [4] which relies on a distributed trust model which enables nodes to monitor their neighbours behaviour. Two features if distributed trust model are used in this scheme; recommendation-based trust and trust-based recommendation. Recommendation on node behaviour is collected from the neighbours' *personal references.* Momani and Challa [5] have introduced a trust model and a reputation based system based on sensed data which is the continuous version of the beta reputation system introduced in [14]. They have used Bayesian probabilistic approach to collect information to establish trust among nodes. A study conducted by Kim and Seo [6] proposes a trust model using fuzzy logic based on the data exchange among nodes which is very much similar to collecting trust votes and establishing reputation of nodes in the network. The reputation is then used to determine the

degree of trust. A group based trust management scheme is presented by Sheikh et al [7], in which a hybrid trust approach is adapted to assign a trust value for the entire group of nodes. Chen et al [8] have proposed a distributed agent-based trust management scheme to consider Packet-Dropping and Hello Flood Attacks to detect the un-trust nodes. They have later introduced a reputation based trust model using probability, statistical and mathematical analysis and have suggested a trust system to build up a reputation and trust space [9]. Marsh [10] has introduced trust management based on a computational model.

The proposed trust based security scheme is based on two trust-based models: CORE, stands for a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, proposed by Michiardi and Molva [11], and RFSN, a reputation-based framework for sensor networks, proposed by Ganeriwal and Srivastava [12]. Both of these models use collaborative monitoring and watch dog mechanisms to establish trust among nodes.

3. THREAT MODEL

Threats in sensor networks can be classified as external and internal. External threats occur from outside the sensor network and may amount to mere passive eavesdropping on data transmissions, but can extend to injecting bogus data into the network to consume network resources and rage Denial of Service (DoS) attacks. Internal threats stem from compromised nodes running un-trust data or from attackers who have stolen the cryptographical contents from legitimate nodes. The proposed framework addresses both internal and external threats.

Roosta et al. [13] have categorised attackers as *mote-class* attackers and *laptop-class* attackers. A mote-class attacker has access to a few motes with the same capabilities as other motes in the network. A laptop-class attacker has access to more powerful devices, such as laptops. This gives the adversary an advantage over the sensor network since it can launch more serious attacks.

An *insider* attack versus an *outsider* attack: An outside attacker has no special access to the sensor network, such as passive eavesdropping, whereas an inside attacker has access to the encryption keys or other codes used by the network. Thus an inside attacker could, for example, be a compromised node which is a legitimate part of the sensor network.

A *passive* attacker versus an *active* attacker: Passive attackers are only interested in collecting sensitive data from the sensor network, which compromises the privacy and confidentiality requirements. In contrast, the active attackers' goal is to disrupt the function of the network and degrade its performance. For example, the attacker might inject faulty data into the network by pretending to be a legitimate node.

4. TRUST MODEL

In sensor networks there are one or more base stations, such as PCs, which are the sinks and aggregation points for the information gathered by the nodes. These base stations are the interface between the sensor network and the user. Since base stations are often connected to a larger and less resource-constrained network, it is generally assumed that a base station is trustworthy as long as it is available. There are no trust requirements placed on the sensor nodes as they are vulnerable to physical capture and other attacks [13].

5. REPUTATION BASED TRUST MANAGEMENT

The proposed reputation-based trust management scheme uses trust vote to establish trust among nodes. Value of trust vote is increased with every successful message transmission from one node to another. This trust value is compromised when a neighbouring node enters a negative vote for a particular node. If the negative vote reaches a pre-determined threshold that node is declared as un-trusted node. In this trust model following tasks are performed:

1. Issuing of a trust vote
2. Maintaining a trust table
3. Reporting an un-trusted node

All the nodes perform the above three tasks. When a Node *A* sends a message to Node *B* first time it creates a *trust table* for Node *A*. When Node *B* transmits the message to the next node, Node *A* listens and compares this message with the one it has sent to Node *B*, thus establishing an original and an actual message. If the message transmitted by Node *B* is the same as the original then node *A* records one trust value for Node *B* and continues this process with every message transmission, hence increasing the trust value for Node *B*; however, if there is a difference between the original and actual messages forwarded by Node *B*, Node *A* enters a negative trust value for Node *B* and continues updating the *trust table*. Once a negative trust vote value reaches a pre-determined threshold then Node *A* declares that Node *B* is un-trusted. Node *A* then broadcasts that negative trust value about Node *B* to other neighbours warning them not to rely on transmission from Node *B*.

Each node builds a *trust table* containing the reputation of nodes in the cluster. Entries in this table contain the node *ID*, and the number of trust and un-trust entries. Nodes update this table every time they observe the message transmission as shown in the Table 1.

TABLE 1: TRUST TABLE

Node ID	Trust entries	Un-trust entries
ID	TE > 1	UE > 1

Each node builds its own *trust table*. Every time a node observes an un-trust entry *UE* it adds into its node trust table but also disseminates this information among its neighbours. Those nodes listening to the message update their *trust tables*. The broadcast message also acts as an inquiry to which the nodes listening reply with their statistics regarding the subject node. Fig. 1 illustrates a clustered sensor network of 100 nodes, having five clusters and a base station. In this figure Nodes *C* and *D* are neighbouring nodes of *A* and *B*; they listen to the transmission from Node *A* and respond with a un-trust

entry if the un-trust count for Node *B* in their *trust table* is greater than its trust count. Fig. 2 (a) shows a message sent by Node *A*, while in Figure 2 (b) shows an altered message from Node *B*. every altered message adds the un-trust entry for that particular node.

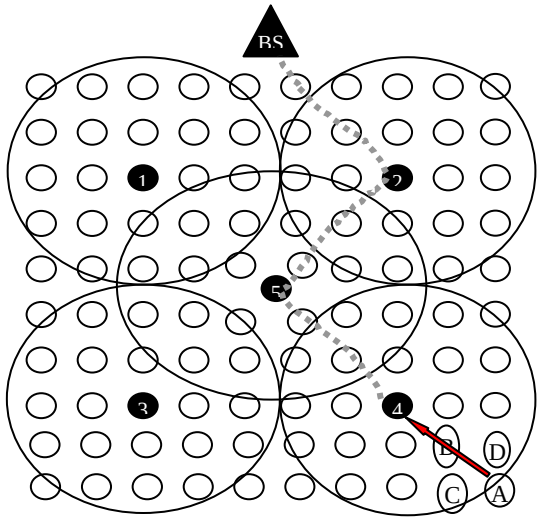

Fig. 1. A typical clustered sensor network, Node *A* send s a message to Node *B*, Node *A*, *C* and *D* create a *trust table* for Node *B*.

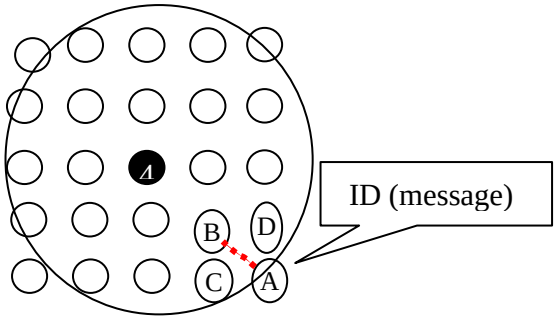

Fig. 2 (a) Message sent by Node A

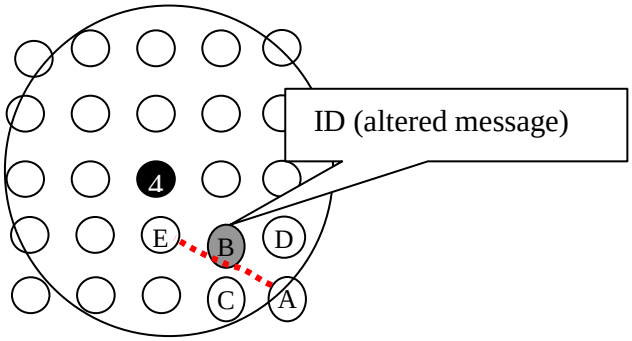

Fig. 2 (b) Message altered by Node B

Node *A* collects the replies from its neighbours and updates its *trust table*, it increases its own trust entry for Node *B* by one and the un-trust entries accordingly.

Once the un-trust entries reach a certain threshold, Node *A* broadcasts that Node *B* is a un-trust node and all the neighbouring nodes update their *trust tables*. When notification of this reaches a cluster leader, it isolates Node *B* from the cluster and discards any messages coming from it. The cluster leader also broadcasts a message saying that node *B* has been isolated, so that any message originated from node *B* is immediately discarded by its neighbouring nodes hence isolating and effectively removing Node *B* from the network.

6. EXPERIMENTAL EVALUATION

This section presents an evaluation of how the reputation and trust based scheme performs in a multi-hop network.

J-SIM was used to simulate the reputation and trust behaviour of nodes. Starting with a scenario of 100 nodes randomly deployed over an area of 100 x 100 metres, a node transmission range of 30m was assumed. One of the nodes was to randomly become un-trust. The scheme works as follows:

Neighbouring nodes monitoring the actual and sent values of data. Whenever any node detects a un-trust node, it increases its *trust table* by 1 and broadcasts a message to inform other neighbouring nodes. Whenever the counter reaches a threshold of 3 for a specific node, its neighbours consider that node is un-trust node.

The sending node stays awake until the receiving node has forwarded the packet. Because of interference, this scenario might not work all the time; therefore, nodes receive a trust value from their neighbours, the threshold for which can be increased or decreased depending on the application.

Each node transfers one packet every 100 seconds. When a node receives a packet not intended for it, it first checks the destination to see whether it is for one of the neighbouring nodes. If not, it discards the packet. The probability that the node stays awake to monitor its neighbours is 50%. If a un-trust node is detected, the detecting node broadcasts the ID of the un-trust node to its neighbours.

Once the cluster leader or base station receive the alert about a un-trust node from at least 3 neighbouring nodes, it declares the node un-trust and isolates it from the network. The cluster leader or base station waits for the alerts from 3 nodes to ensure that the un-trust node itself is not generating an alert about the legitimate nodes.

The level of this scheme's security depends entirely on the application. The percentage of neighbours being awake all the time could be 100 percent thus providing complete security. Instead, in order to be more energy efficient, the topology works by letting each node go to sleep when it is not sending or receiving a packet.

As seen from the experimental results shown in Fig. 3, the time required to detect un-trust node decreases when the

number of nodes in the network is increased. This is because in dense network, the probability of un-trust node detection is higher and faster because there are more neighbours monitoring the nodes. The results in Figure 3 are an average of 10 runs.

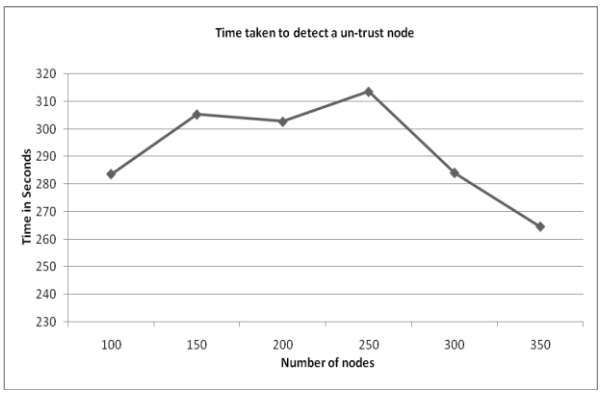

Fig. 3 Time taken to detect a un-trust node

In using the reputation and trust management to detect trust behaviour, and on the basis of the responses from other neighbouring nodes, if the number of trust entries concerning a particular node reaches a set threshold, that node is declared un-trust. This message is broadcast, alarming all the neighbours and eventually reaching the base station. The cluster leader or base station then isolates the un-trust node and all traffic coming from that node is ignored. The simulation results show that the time it takes to detect a un-trust node is decreased when there are more nodes in the network, and that it provides a fast and efficient way to detect un-trust nodes.

7. CONCLUSION AND FUTURE WORK

This preliminary work will set a base to strengthen the security framework by integrating the reputation and trust management mechanism. This will be achieved by modelling wireless sensor networks as reputation and trust based systems. Extensive simulation and experiments on sensor nodes will be performed to establish a trust relationship among the nodes. Choosing relay nodes to forward the packets to other nodes will be based on the trust value calculated by a voting phenomenon from the neighbouring nodes. Relaying of packets will be protected by a secure key management scheme. This will provide not only the capability of informed decision making but also extended security in wireless sensor networks.

REFERENCES

[1] T.A Zia and A.Y. Zomaya, A security framework for wireless sensor networks, in the proceedings of IEEE Sensor Applications Symposium (SAS06), February 7-9 2006, Hoston, Texas, USA.

[2] A. Boukerche, and X. Li, An agent-based trust and reputation management scheme for Wireless Sensor Networks. In IEEE Globecom 2005.

[3] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, Highly reliable trust establishment scheme in ad hoc networks. Journal. of Computer Networks, p. 687–699, 2004.

[4] Y. Zhiying, K. Daeyoung, L. Insun, K. Kiyoung, and J. Jongsoo, A security framework with trust management for sensor networks, 1st Inl Workshop on Security and Privacy for Emerging Areas in Communication Networks, 5-9 Sep 2005.

[5] M. Momani and S. Challa, Trust management in wireless sensor networks, in the proceedings of 5th ACM Conference on Embedded Networked Sensor Systems (SenSys 2007), November 6 – 9, 2007, Sydney, Australia.

[6] T. K. Kim, and H. S. Seo, A Trust Model using Fuzzy Logic in wireless sensor network. Proceeding of World Academy of Science, Engineering and Technology. Vol. 32, August 2008. ISSN 2070-3740.

[7]R. A. Sheikh, H. Jameel, S. Lee, S. Rajput, Y. J. Song, Trust management problem in distributed wireless sensor networks, proceedings of the 12th IEEE International Conference on Embedded and real-Time Computing Systems and Applications, August 16-18, 2006, Sydney, Australia.

[8] H. Chen, H. Wu, J. Hu, C. Gao, Agent-based trust management model for wireless sensor networks," *MUE*, pp. 150-154, The 2nd International Conference on Multimedia and Ubiquitous Engineering (MUE 2008), April 24-26 2008, Busan, Korea.

[9] H. Chen, H. Wu, X. Zhou, and C. Gao, Reputation-based trust in wireless sensor networks, *MUE*, pp. 603-607, 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), 2007.

[10] S. Etalle, and S. Marsh, Trust management, proceedings of IFIPTM 2007: Joint iTrust and PST Conferences on Privacy, Trust Management and Security, July 30-August 2, 2007, New Brunswick, Canada. IFIP International Federation for Information Processing 238. Springer Verlag, Berlin.

[11] P. Michiardi and R. Molva, CORE: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. Communication and Multimedia Security, September, 2002.

[12] S. Ganeriwal and M. Srivastava, Reputation-based framework for high integritysensor networks, in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), October 2004 pp. 66-77.

[13] T. Roosta, S. Shieh, and S. Sastry, Taxonomy of security attacks in sensor networks and countermeasures. Berkeley, California, University Press.

[14] A. Jøsang and R. Ismail, "The BetaReputation System," in *15th Bled Electronic Commerce Conference*. Bled, Slovenia, 2002.