International Journal of Security and Its Applications
Vol. 3, No. 2, April, 2009

Task-based Trust Management for Wireless Sensor Networks

Haiguang Chen
Dept of Computer Science, Shanghai Normal University
chhg@shnu.edu.cn

Abstract

Cryptography and Authentication is the traditional approach to provide security in WSNs(Wireless Sensor Networks). However, that conventional approach is not sufficient for the unique characteristics and novel misbehaviors encountered in WSNs. In this paper, we use a general tool which has been used in economics, statistics and data analysis. With this approach, we propose a task-based trust management framework for WSNs where nodes maintain reputation for other nodes of several different tasks and use it to evaluate their trustworthiness. We show that this framework provides a scalable, diverse and a generalized approach to recognize all types of misbehavior resulting from malicious or faulty sensor nodes. Our framework has more simple trust computation than ATSN and more suitable for scarce power resource nodes. The simulation results and analysis show that our framework can detect the malicious nodes fast if having abnormal result while doing certain task with other nodes.

1. Introduction

WSNs is vulnerable to attack due to the nature of the wireless media and restricted resource. There are several proposed protocols such as authentication, encryption and IDSs[3,5,7] that provide the security of WSNs. But those scheme cannot detect some new kind of attacks or the computation is too heavy for the restricted resource node.

Trust-based secure mechanism in WSNs[2,6] has been presented, recently. The node observes the behavior of other nodes, then it can get reputations and trust rating about other nodes. But in[2,6],the authors don't distinguish the different task while cooperating with other nodes.

In this paper, we propose a task-based trust framework for Sensor Networks (TTSN) The sensor node has different trust rating for different task while cooperating with other nodes. The node considers the trust rating to decide whether to cooperate with other nodes to finish a certain task. Our model use watchdog scheme to observe the behavior in different task of these nodes and broadcast their trust ratings. The main contributions in this paper are listed as follows:

A. Offer a novel novatal distributed task-based trust framework to detect malicious or faulty nodes for different task in Sensor Networks.

B. Provide a TTSN protocol to deal with the malicious sensor nodes in different event.

C. Simple computation of trust and utmost to cooperate with other nodes.

This Paper is Supported By Innovation Program of Shanghai Municipal Education Commission and the Project number is 09YZ154

The rest of the paper is organized as follows. Section 2 briefly describes the related works about security in WSNs and Ad-hoc networks. Section 3 describes the task-based trust model. Section 4, the implementation of task-based trust framework model is described and simulation results are shown. The conclusion is drawn in section 5.

2. Related Works

This section will briefly introduce some security works about reputation and trust system in WSNs. The reputation and trust systems have been proved useful mechanism to address the threat of compromised or faulted entities in sensor networks. They operated by identifying selfish peers and excluding these entities from the network.

DRBTS [8] is a special case to build a distributed model in location-beacon sensor networks using both first-hand and second-hand information. CONFIDANT [1] is a routing protocol in MANETs which is a distributed, symmetric reputation model using both first-hand and second-hand information for updating reputation values. However, they easy to be bad-mouth attack if we use second-hand information, and most of the trust system is unsymmetrical.

ATSN [3] is an agent-based trust model for WSNs, but it cann't distinguish different tasks which effect the trust rating, and all the tasks has the same affects. Each sensor node has one trust rating value for different tasks, that scheme is not suitable for WSNs due to its constrained resource. And the computation is too heavy for sensor nodes.

RFSN[4] is the first reputation and trust-based model designed and developed exclusively for sensor networks, which using watchdog mechanism to build trust rating. But the watchdog cannot record all the behavior due to its own fault, so there is uncertainty in the trust system.

In this paper, we propose a TTSN protocol to detect the malicious or faulted nodes in different tasks. The focus of our work is to build a distributed task-based trust framework in WSNs.

3. Task-based Trust Framework

Establishment of trust-based security in WSNs requires successful detection of the intruders and discarding them. However, if we don't distinguish the different task of a node, we may arrive at wrong evaluation of trust. In fact, a node in WSNs not only send packets but also collect some data to cooperate with its neighborhood node. As a consequence, collaboration between neighboring nodes is required. And a node can do several tasks to cooperate with other node. A neighborhood node may do badly in task TA_{Ti}, but may do perfectly in task TA_{Tj} with a node. In our scheme, every node in the network monitors the behavior of its neighbors about different task, and upon detecting abnormal action from any of them. If the trust rating about a certain task TA_{T1} of a sensor node is too low, then its neighborhood node may stop cooperating to finishing the task TA_{T2} with it. It means the node was discarded by another node about task TA_{T2} ,but the node can still cooperate with it about other tasks. Our mechanism builds trust through an entity, called the Task and Trust Manager Module that runs on each node in the sensor network. The Task and Trust Manager Module involves three

main components: (1) monitoring module; (2) reputation handling module and (3) task and trust handling module.

3.1 The Monitoring Module

Every node independently monitors the packet forwarding activities of its neighbors. All of these packets were related to the set of task $TA = \{TA_{T1}, TA_{T2}, ..., TA_{Tn}\}$.These tasks were done by nodes among neighbors. A node can do several tasks with other node in its one-hop neighbors. This monitoring is related to the proportion of correctly done a certain task TA_{Ti} with respect to the total number of task TA_{Ti} during a fixed time window. And the monitoring module can classify different packet forwarding activities relate to different task. Based on these statistics, if an anomaly result about a certain task is detected, the monitor informs the task and trust handling module, which analyses the different task of nodes and its trust rating.

3.2 Reputation Handling Module

The main functionality of the reputation handling module is getting the different output value for different task.

Def 1: The task set TA done by sensor nodes.

Let $TA=\{TA_{T1}, TA_{T2}, TA_{T3}, ...TA_{Tn}\}$ (1)

Different nodes have different performance while doing these tasks, we use task function to score the performance.

Def 2: Task function for different task.

$$F_{TA} = \{F(TA_{Ti}) \mid \forall TA_{Ti} \in TA, F_{TA}(TA_{Ti}) \geq 1, F_{TA}(TA_{Ti}) \in N\} \quad (2)$$

When a sensor node A does a task, TA_{Ti} ,for another node B .the sensor node B can get two kinds of different outputs to evaluate the performance of the node A after finishing the task TA_{Ti} .One is negative, the other one is positive. We use p_i refer to positive outputs value; n_i refer to negative outputs value, respectively. All of these p_i and n_i satisfy the following formula.

$$p_i = F(TA_{Ti}) \text{ or } n_i = F(TA_{Ti}) \text{ , } \underset{i=1}{\overset{n}{p_i}} \cup \underset{i=1}{\overset{n}{n_i}} = F(TA_{Ti}) \quad (3)$$

We use $< p_i, n_i >$ to denote the reputation value while doing task TA_{Ti} . $< p_i, n_i >$ is the binary event for a certain task TA_{Ti} of sensor node.

3.3 Trust Handling Module

We will build task-based trust managemnet system, which based on a Bayesian formulation, being developed for resource constraint sensor nodes within the framework of TTSN.

According to the Bayes theorem, $P(S_i \mid T) = \frac{P(S_i)P(T|S_i)}{\sum_{i=1}^{\infty} P(S_i)P(T|S_i)}$ and the Beta Distribution, we get the following definition of conditional probability.

Let x be the probability of a positive outcome. The posterior probability of reputation $< p, n >$ is the conditional probability of x given $< p, n >$ [2].

Def 3: Define the probability of a positive outcome, x

$$P_{<p,n>}(x) = P(x \mid < p, n >) = \frac{P(<p,n>|x)P(x)}{\sum P(<p,n>|x)P(x)} = \frac{(p+n+1)!}{p!n!} x^p (1-x)^n = Beta(p+1, n+1) \quad (4)$$

The trust metric of a node about the task TA_{Ti} is the statistical expectation of the posterior probability function and is given by:

$$T_{TA_{Ti}}^{A,B} = E(P(x)) = E(Beta(p_i + 1, n_i + 1)) = \frac{p_i + 1}{p_i + n_i + 2} \quad (5)$$

Where $T_{TA_{Ti}}^{A,B}$ means the trust rating of node A about task TA_{Ti}, which stored in the memory of node B.

Our TTSN framework model uses the following equation to update the trust rating of sensor nodes for different task:

$$T_{TA_{Ti}}^{A,B} = \gamma T_{TA_{Ti}}^{A,B(curr)} + (1 - \gamma) T_{TA_{Ti}}^{A,B(newg)} \quad (6)$$

Where γ is an aging factor, it can take a value in the interval [0, 1]. The value $T_{TA_{Ti}}^{A,B}$ is a weighted sum of two components. The first part describes the sensor node's trust rating already present in the trust table of sensor node about task TA_{Ti}. The second part reflects contribution of sensor node's new trust rating value about task TA_{Ti} in fixed time window. As a sensor node's previous trust rating is also considered, the evaluation of trust rating will be more consistent and seamless.

4. Experimental Results

Our simulator is composed of the following modules: the sensor nodes, the intruder nodes, the traffic data and the events generator. If an event happened then these sensor nodes will execute tasks such as data collection, data route, neighbor found, time-synchronization and location report among neighborhood. In our simulator, we only consider the one-hop neighbor nodes. For these nodes is direct partner to finish a certain task. The behavior of intruder nodes can good or bad at any moment to different tasks. The intruder nodes except take on-off attack [6], and take the following attack: The intruder cooperates with the node A, when the intruder executes task TA_{Ti}, its performance well; when the intruder executes task TA_{Tj}, its performance bad.

We use the following metrics to evaluate our TTSN framework.1) The time to detect malicious behave of sensor nodes and 2) the lifetime of the whole WSNs.

We consider a network scenario where the sensor nodes and the intruder nodes are scattered randomly to monitor the object of a terrain. These nodes cooperate with each other to finish some tasks among them.

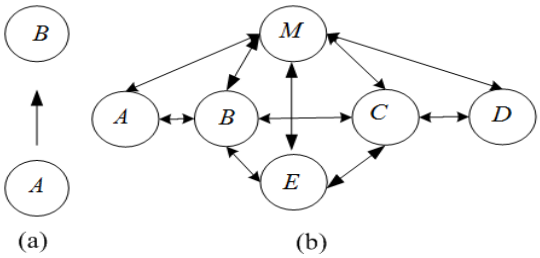

Figure 1. Network Setup

(a): We consider node A and B, shown in Figure 1(a). The node B is a malicious node. The node B executes several tasks with the node A, such as date collection, packet forward and time- synchronization. The node B does well in data collection and time- synchronization, but does badly in packet forward. In this case, we will use RFSN [4] and TTSN to detect vicious behave of the node.

(b): these sensor nodes M, A, B, C, D, E cooperate with each other to form a neighbor area. In RTSN and ATSN [6], if the trust rating of a sensor node is low enough that its neighbor node will exclude it from the networks. But our TTSN is a different scheme from them. For example, if the trust rating of a malicious node about task TA_{Ti} is every low and the other node don't cooperate with it for task TA_{Ti}. But the other nodes can still cooperate with it for other task TA_{Tj}.In this case, we will consider the lifetime of the neighbor area formed by nodes M, A, B, C, D, E with different trust scheme.

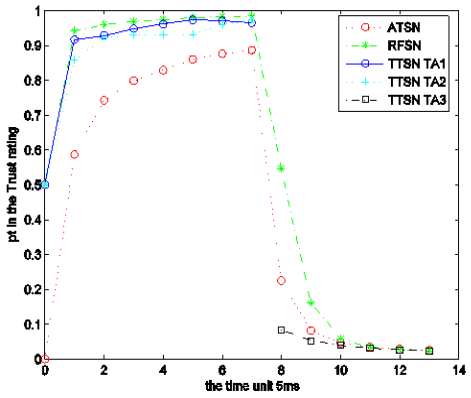

Figure 2. ATSN, RFSN VS TTSN with a=0,2

Figure 2 is the simulation result of Figure 1 (a). In the first 7 slices, the node B does well in task TA_{T1}(date collection) and TA_{T2}(time-synchronization), so the trust rating of them are high, the node A can cooperate with node B. But the trust rating of task TA_{T3}(delivers packet for node A.) is low. In our TTSN, the node can continue

cooperate with node B in the task TA_{T1} and task TA_{T2}.But both ATSN and RTSN cannot cooperate with the node B due the low trust rating.

Figure 3 is the simulation result of Figure 1 (b). From the figure 3, we get in RFSN, the energy is consumed fast because some of the sensor nodes were exclude from the neighbor area, so no other node cooperate with them. But in our TTSN, due the trust rating base on different task, if some of the sensor nodes cannot cooperate with them on some tasks, they still can cooperate with theirs neighbor nodes in other nodes. They still can work in the area.

5. Conclusion

We propose a TTSN framework model to enforce the security of WSNs, in this paper. The scheme is distributed and the sensor node build trust rating by their own observation in different task. Our TTSN scheme is more suitable for trust system in WSNs due to its trust system build on different task. A sensor node has several trusting rating in WSNs. The scheme can be used in large scale WSNs. With the growing importance of sensor network applications, our scheme helps to provide a more accurate guarantee along with cryptographic mechanisms of the actual time to detect the malicious behavior in different task of WSNs.

References

[1]S. Buchegger and J.-Y. Le Boudec. “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks)”.Proceedings of MobiHoc 2002, Lausanne, CH, June 2002.
[2]JGeorge Casella and Roger L. Berger. Statistical Inference. Duxbury Press, 1990.
[3] Dimitriou, T., Krontiris, I.: Secure In-network Processing in Sensor Networks. In:Security in Sensor Networks. CRC Press PP275-290 (2006)
[4]S.Ganeriwal and M. Srivastava. “Reputation-based framework for high integrity sensor networks”. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), pp. 66-77, Oct 2004.
[5] S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, 2006.
[6]Haiguang Chen, Huafeng Wu , Xi Zhou, Chuanshan Gao Agent-based Trust Model in Wireless Sensor Networks. 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007) PP 119-124,July 30 - Aug 1, 2007 Qingdao,China.
[7] Krontiris, I., Dimitriou, T., Freiling, F.C.: Towards intrusion detection in wireless sensor networks. In: Proceedings of the 13th European Wireless Conference, Paris,France (April 2007)
[8]S. Buchegger and J.-Y. Le Boudec. “Self-policing mobile ad-hoc networks by reputation systems”. IEEE Communications Magazine, July 2005.

Authors

Haiguang Chen

is Ph.D Candidate in the Department of Computer Science and Engineering at Fudan University. And he is a professor of ShangHai Normal University. During 2006-2007, he was a visiting scholar in Dept. of IST at Weber State University, UT, USA His research interests include Wireless Sensor Networks, Mesh networks and the security of networks.