RASN: Resist on-off Attack for Wireless Sensor Networks

Pengzhi Shi
Department of Computer Science
Shanghai Normal University
Shanghai, China, 200234
Shipengzhi1986@126.com, 2nd

Haiguang Chen
Department of Computer Science
Shanghai Normal University
Shanghai, China, 200234
chhg@shnu.edu.cn

Abstract—**Reputation Based Framework for Wireless Sensor Networks(RFSN) represent soft security mechanisms that complement traditional information security mechanisms. RFSN can prevent malicious of data from internal adversaries or faulty nodes. In this paper we add a new architecture called Trust-Holding-Agent (THA) to build a new Trust Framework model (RASN) improve on RFSN. The new framework model will be more suitable for wireless sensor networks. In addition, RASN is effective in resisting the On-Off Attack. The simulation results and analysis show that our scheme not only can fast detect the malicious nodes of On-off attacks, but also have incentive and punitive mechanism.**

Keywords-Wireless Sensor Networks; Reputation; Bayesian Formulation; Revision Algorithm; On-off Attacks

I. INTRODUCTION

With the wide applications of Wireless sensor networks (WSNs), people find the security of WSNs is ever more important. The traditional method of network security is to resort to such tools as cryptography and authentication. However, we find that this security mechanism cannot prevent malicious or non-malicious insertion of the data from internal adversaries or faulty nodes.

In fact, the challenge that sensor networks security faces relying on the inherent collaboration between network nodes to accomplish the planned functionalities. Therefore, establishing and quantifying trust is an important means of network security. The Reputation based Framework for Sensor Networks (RFSN) was proposed by S. Ganeriwal [2].

In this paper, we add a new architecture called Trust-Holding-Agent (THA) to RFSN. This new trust framework model is called Reputation Agent Based Framework for Wireless Sensor Networks (RASN). THA contains a trust evaluation revision algorithm to improve on RFSN. The main contributions in our paper are listed as follows:

Improve the RFSN trust framework model's ability of detecting malicious sensor nodes when it is under the On-Off Attack.

Develop an incentive and punitive mechanism in reputation system for WSNs.

The On-off Attacks of trust/reputation systems are extensively studied and protection strategies are proposed.

The rest of the paper is organized as follows. Section II presents the related works about RFSN. Section III detailed describes the RASN and trust evaluation revision algorithm. In Section IV, On-off Attacks and protection techniques for WSNs is introduced. Simulation results are shown in Section V, followed by the conclusion in Section VI.

II. RELATED WORKS

At present, a lot of reputation mechanisms are proposed and studied. An overall survey of the reputation system in AD-HOC networks and a more detailed overview has been established in [5].

Trust-management approach of distributed systems security was first put forward in an article on the shortcomings of traditional cryptographic mechanisms. In this field, some early efforts were made by KeyNote [4] and RT framework. From then on, the established reputation systems based on trust management have been studied and applied to different fields such as human social networks, ecommerce, peer-to-peer networks etc.

RFSN was the first reputation-based model designed and developed for sensor networks. RFSN has borrowed some of the design features the current work has worked out, but at the same time it differs from all of the present reputation-based systems, such as: eBay [6], peer-to-peer networks [7] etc. All of them are confined to a certain area or different architecture.

In this paper we join a new Architecture called Trust-Holding Agent (THA) to calculation and conserve in RFSN. The THA propose a trust evaluation revision algorithm to get the final trust value.

III. TRUST FRAMEWORK MODEL

In section 2, we have described some related research work on reputation and trust system in WSNs. S.Ganeriwal, et al [2] build reputation Rij , and then get the trust Tij=$\frac{\alpha + 1}{\alpha + \beta + 2}$.If i and j had been a lot of good interaction, then α's value is very large. Suddenly, the system is attacked by attack. β' s value began to increase, but Tij's value is still very close to 1 at this time. This results indicate that RFSN detect the malicious nodes of On-off attacks are not sensitive enough. So we propose a trust evaluation revision algorithm to solve the problem.

In RFSN, when a node inquires other nodes in the network, it aims to obtain the trust value of the target node. The target node, if it is malicious, will attack other nodes as a way of revenge or try to prevent them from revealing the bad information after it finds a report on its bad value given by other nodes. Anonymity is one way to cope with this problem. Therefore, we use a fixed server computer to manage the trust value of these nodes. As this server computer is anonymous, other nodes cannot recognize its identity. We name it THA. The function of THA is to calculate, aggregate and conserve reputation information of nodes.

A. Architecture

Every node stores a trust table of other nodes which interact with it directly and indirectly. RASN differs from RFSN , RASN stores the consolidated value of the direct and indirect trust value. The THA uses a trust evaluation revision algorithm to deal with all kinds of reputation value and achieve a final value. Figure 1 depicts the RASN.

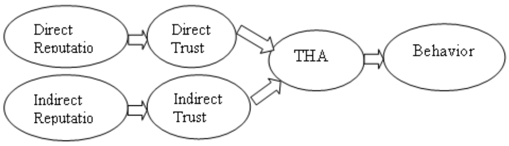

Figure 1. Architectural Design of RASN

Reputation Table is maintained as a probabilistic distribution, enabling the node to have full freedom. Trust Table is a subjective expectation about a node's prediction of another node's future behavior. In RASN, this is obtained by taking the statistical expectation of the probability distribution representing the reputation between the two nodes. The function of THA will be described in detail in Section 3.2.

B. Trust-Holding-Agent

THA collects Direct and Indirect Trust of node i and j from Trust Table. Then THA get new Trust value, as show in equation (1):

$$(T_{ij}^{new})\mathrm{D} = f[\theta, (\mathrm{Tij})\mathrm{D}];\ (T_{ij}^{new})\mathrm{ID} = f[\theta, (\mathrm{Tij})\mathrm{ID}] \quad (1)$$

Here, θ is described as a revision factor, that comes from the reputation change. The account of (T_{ij}^{new})D and (T_{ij}^{new})ID which we will describe in section 3.3.2 and 3.3.3 respectively.

The following we survey the relevant results of Kempe et al. [8].

C. Revision Factor

As the proposed reputation model intends to have incentive and punitive mechanism and fast detect the malicious nodes of On-off attacks. First, we introduce the concept of Latest Times of Trust Mutation (L) and Revision Factor θ.

Definition 1. LM is an integer variable, which records the times of Trust Mutation that a change between a current trust value and the average of previous trust values.

L has different meanings for Direct and Indirect Trust Value, is expressed {(L)D,(L)ID} respectively.

Definition 2. Θ is a monotonic increase function, which maps the nodes' L to a real value θ= [0, 1].

$$\theta=\Theta(L)=\frac{a\tan(L-\mu)+a\tan(\mu)}{\pi/2+a\tan(\mu)} \quad (2)$$

where parameter μ> 0 is the threshold controlling when the value of Θ function increases quickly. The value of Θ function increases slowly when L is less than parameter μ, then increases quickly and close to 1 when L is large enough.

D. Direct Revision Trust

The Let the set of times be N = {1 . . . n}. Node i hold a number $T_{ij}^{k} \in [0, 1]$ for node j (k ∈ N). This number represents j's reputation with respect to i in the k times. Let $\overline{T_{ij}} = \frac{\Sigma_k T_{ij}^k}{k}$ is the average of j's trust from 0 to k times. $\overline{T_{ij}}$ denote the average result of the direct experiences of node i on node j up to now.

The T_{ij}^{new} aren't complete adopted, but T_{ij}^{new} are only accepted if the reported trust does not deviate too far from the average trust $\overline{T_{ij}}$ and was reworked by revision algorithm. This deviation and revision degree is controlled by the deviation degree d^k and parameter D^k for the k moment interaction:

$$d^k = \left| T_{ij}^{k} - \overline{T_{ij}} \right|;\quad D^k = T_{ij}^{k} - \overline{T_{ij}} \quad (3)$$

The variety of Tij and $\overline{T_{ij}}$ have only two possible states: Tij is continuous increasing or decreasing sequence, the trust is non-continuous---meaning that sometimes Tij is larger than $\overline{T_{ij}}$ and sometimes Tij is less. We note times of trust Mutation as Continuous Mutation times (L)c and Non-Continuous Mutation times (L)nc respectively. (L)c, is build up using current trust compare with previous trust, (L)nc, is build up using the derivative of current trust compare with the derivative of previous trust. The method will be given in Algorithm 1.

```
Judgment Mutation Times
    Assumptions j's reputation with respect to i always increase
    If $T_{ij}^{k} - T_{ij}^{k-1} < 0$   //current trust less than previous trust//
    (L)c =(L)c +1
    Else (L)c unchanged, End if
    The derivative of k-times trust, $C_{ij}^{k} = -\frac{\alpha_j^k\beta_j^k + \alpha_j^k}{(\alpha_j^k + \beta_j^k + 2)^2}$
    If ( $C_{ij}^{k+1} - C_{ij}^{k}$ )*( $C_{ij}^{k} - C_{ij}^{k-1}$ ) <0      //a turning point in derivative sequence of trust//
    (L) nc = (L) nc +1
    Else (L)nc unchanged, End if   (L)D =max {(L) c, (L) nc}
    End judgment
```

Then substituting Definition 2 will calculate Revision Factor θ. The T_{ij}^{new} of calculating method is proposed in Algorithm 2. Finally (T_{ij}^{new})D= T_{ij}^{new}

```
Procedure Revision
    If $D^k$>0      $T_{ij}^{new}$ = Tij –θ*d
    Else $T_{ij}^{new}$ = Tij +θ*d
    End procedure
```

Published by Atlantis Press, Paris, France.

E. Indirect Revision Trust

The method of calculate (T_{ij}^{new})D and (T_{ij}^{new})ID is very similar, the difference is (L)ID. The value of T_{ij}^{k} with the k-time indirect trust express that node i receives trust information about node j through node k, but not through k-times time. We account for revision factor θ so that the system gradually forgets about false trust.

The range of possible values of d^k is divided into ten intervals(or bins), bin1=[0,0.1], [0.1,0.2] … , bin10=[0.9,1] , the corresponding values of (L)ID are 0, … ,9 respectively. For example, if d^k equal to 0.68, thus (L)ID equal to 6 with the values of d^k in bin7. It must be modified and approach to the average trust as much as possible. Then, calculating Revision Factor θ and T_{ij}^{new} 。

IV. Attacks and Protection

We will show simulation result in section 5.First of all, we will present the On-off attacks and defense methods in our model.

WSNs are often suffer from different types of attacks, such as bad mouthing attack, On-off attack, Conflicting Behavior attack. On-off attack means that malicious entities behave well and badly alternatively, hoping that they can remain undetected while causing damage. The attacks have only two possible states: either the attack is on, meaning that some action is being performed on a specific node, or the attack is off, meaning that the node is left to operate as normal.

The value of Trust is dynamic. A good entity may be compromised and turned into a malicious one, while an incompetent entity may become competent due to environmental changes.

RASN can defense against On-off Attacks, we use a simple threshold based policy to decide attacks. Once the system is decided to be attacked, L is equal to 0 and is recount. {Attacks if L ≥TH ; Don't attacks if L ＜TH}

V. Simulations

We consider sensor nodes are scattered randomly. We use the trust between nodes i and j, Tij, as a metric for analyzing the efficacy of RFSN and RASN. Node i initializes the two reputation parameters of node j, αj and βj, to 0, thereby the initial trust metric, Tij, is 0.5. For each data packet that is successfully forwarded by node j, node i assigns a positive rating of (1,0) and assigns a rating of (0,1) otherwise.

Let us consider three different phases in the process of THA collecting data: (1) Node j fully cooperates and forwards every packet of node i (2) Node j is attacked by On-off Attack (3) Resume to node j fully cooperates. In order to study easy, we require the proportion of On and Off randomly generated. Figure 2 shows the contrast between RFSN and RASN with direct trust.

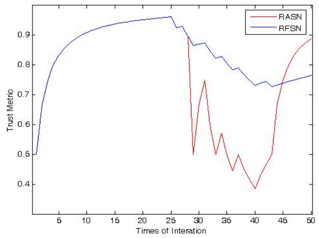

Figure 2. Effect of on-off for direct trust

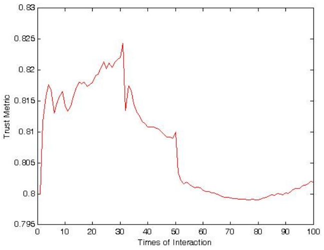

Figure 3. Effect of on-off for indirect trust

In Figure 2, The threshold for classifying nodes as good and bad is randomly fixed to be 0.8. For RASN, the new trust value is less than 0.8 in 23-times, thereby node i conclude that node j is malicious. Then node j is punished and always maintained at a very low level. For RFSN, in 26-times. Therefore our scheme can faster detect the malicious nodes of On-off attacks. When the attack stops, RASN model encourages the trust value of node j to fast increase and return to 0.8 in 43-times, but RFSN doesn't.

Then we consider the indirect trust status, the result is seen in Figure 3. When the system is attacked, RASN makes the indirect information from indirect trust table to be close to the average trust, to minimize the probability of influence with the malicious node. The simulation result shows that our framework still keep a high trust level (above threshold 0.8) when it was attacked by On-off .

VI. Summaries

In this paper, we propose the Reputation Agent Based on trust framework model to enforce the security of WSNs. Our RASN will be more suitable for wireless sensor networks due to its THA mechanism and revision algorithm.

Although the reputation system protects nodes' identities, a malicious or failure THA can disseminate false trust information for a node. Remaining problems include preventing malicious computer from becoming THA and preventing nodes from reporting a wrongful trust value for another node. Therefore, we choose good TAH as much as possible.

Our future work focuses on: we are working toward implementing the RASN into defense against other Attacks such as Bad Mouthing Attack and Conflicting Behavior Attack.

The research work in this paper was sponsored by the Innovation Programs of Shanghai Municipal Education Commission and the project numbers are 09YZ154

REFERENCES

[1] H. Chan and A. Perrig, “Security and privacy in sensor networks,” IEEE Computer, vol. 36, no. 10, pp. 103–105, 2003.

[2] 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.Computer, vol. 36, no. 10, pp. 103–105, 2003.

[3] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In Proceedings of IEEE Conf. Security and Privacy, 1996, Oakland, California, USA.

[4] M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis. RFC2704 - The KeyNote Trust Management System Version 2. 1999.

[5] S. Buchegger and J.-Y. Le Boudec. Self-policing mobile ad hoc networks by reputation systems. IEEE Communications Magazine, 43(7):101–107, July 2005.

[6] P. Resnick, R. Zeckhauser. Trust among strangers in Internet transactions: Empirical analysis of eBay’s reputation system. NBER workshop on empirical studies of electronic commerce, 2000.

[7] L. Xiong, L. Liu. A reputation-based trust model for peer-to-peer ecommerce communities. IEEE conference on ecommerce,2003.

[8] Huaizbi Li and Mukesb Singbal. Trust Management in Distributed Systems. Pubilshed by the IEEE Computer Society. pp. 45-53,Feb 2007

[9] A. Jsang and R. Ismail. The Beta Reputation System. In Proceedings of the 15th Bled Electronic Commerce Conference, June 2002.

[10] Kempe, D., Dobra, A., & Gehrke, J. (2003).Gossip-based computation of aggregate information. In FOCS’03: Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (p. 482). Washington, DC: IEEE Computer Society. ISBN: 0-7695-2040-5.