International Journal of Multimedia and Ubiquitous Engineering
Vol. 2, No. 4, October, 2007

Reputation and Trust Mathematical Approach for Wireless Sensor Networks

Haiguang Chen[1,2], Gangfeng Gu[1] , Huafeng Wu[2], Chuanshan Gao[2]

[1]Mathematic and Science College,Shanghai Normal University,Shanghai, P. R. China, 200234
[2]Dept. of Computer Science and Engineering, Fudan University, Shanghai, P. R. China, 200433
[1]{Chhg, gangfeng}@shnu.edu.cn, [2]{hgchen, wuhuafeng ,cgao}@fudan.edu.cn

Abstract

In Wireless Sensor Networks (WSNs), these sensor nodes cooperate with each other to form a network without using any infrastructure. WSNs has a wide application. But the security of WSNs is still an important issue. Some existing approaches mainly rely on cryptography to ensure data authentication and integrity. These approaches only address part of the problem of security in WSNs. However, these approaches are not sufficient for the unique characteristics and novel misbehaviors encountered in WSNs. Recently, the use of reputation systems has become an important mechanism in WSNs. In this paper we propose a reputation and trust mathematical framework for WSNs which borrows tools from probability, statistics and mathematics analysis. We have suggested a new term certainty used in trust system and we argued that the positive or negative outcomes for a certain event is not enough information to make a decision in WSNs. We build up a reputation space and trust space in WSNs, and define a transformation from reputation space to trust space. Finally, we discuss some important properties of them and provide a basement in the trust and reputation for future research in WSNs. And we point out some open problems in reputation and trust system in WSNs.

1. Introduction

Wireless sensor networks (WSNs) have been used increasingly in every type of environment due to their easy of deployment. WSNs provide their users with fast and easy access to their data and services anytime and anywhere, especially in remote area such as battlefield, forest and volcano. Wireless sensor networks serve to collect data and to monitor and detect events by providing coverage and message forwarding to base station. However, the inherent characteristics of a sensor network limit its performance and sensor nodes are envisioned to be low-cost. An adversary can control a sensor node undetectably by physically compromising the node and use the captured nodes to inject faulty or false data into the network system disturbing the normal cooperation among nodes. Authentication and cryptographic mechanisms alone cannot be used to full solve this problem because internal adversarial nodes will have valid cryptographic keys to access the other nodes of the networks.

Besides the node malicious attacks, the nodes are also vulnerable to system faults for low-cost hardware of these nodes. For example, the radio or sensor hardware maybe faults and these nodes cannot perform well or misbehavior in the system for cooperation in monitoring

the event. So this kind of faults cannot be done by authentication and cryptographic mechanisms.

A new kind of mechanism for security has been presented in wireless sensor networks, recently, which borrows tools from economics, statistics and mathematics analysis with cryptography. Basing on the node's observation, these nodes collect some experiences about other nodes' just as existing human societies in the real world. And they can build a trust system based on their experiences. But existing mechanism about trust system in wireless sensor networks has ignored an important thing. The experience may not full be recorded by nodes due to heavy traffic, packets lost or faults of cheap hardware in wireless sensor networks. So there must have some uncertainty in trust and reputation system in wireless sensor networks. And we will describe detail in section 2 and section 3.

In this paper, we use watchdog mechanism to get the experience about other nodes, and build reputation system. Using the node's reputation, we get the trust for the neighbor nodes among its radio range.

The main contributions of this paper are listed as follows:

1. We use watchdog mechanism to present reputation space and then get trust space in wireless sensor networks.
2. We defined a transformation which from reputation space to trust space.
3. We discussed some important properties about the reputation space, trust space and the transformation.
4. We presented some open problems in reputation and trust systems for wireless sensor networks

The rest of the paper is organized as follows. Section 2 briefly describes the related work about security and reputation system in wireless sensor networks. Section 3 describes the mathematical model of certainty for wireless sensor networks used in our paper. Section 4 presents some important properties of the certainty. Section 5 describes some open problems in reputation system and research direction about reputation system in wireless sensor networks and we give our conclusion in section 6.

2. Related works

If we have no adequate security, the applications about wireless sensor networks could be curtailed. Several proposals have been existed, but all of the schemes based on cryptography to ensure secure communication among these resource constrained wireless nodes [7, 8, 9, 10, 11, 12, 13]. And some IDSs have been used for security in wireless sensor networks [14, 15, 19]. But both cryptography and IDSs cannot sufficient for the unique characteristics and novel misbehaviors encountered in wireless sensor networks.

The trust-management approach for security in distributed systems [16] was first introduced in the context of Internet and as an answer to the inadequacy of traditional cryptographic mechanisms for security. Recently, the reputation system and trust has been introduced to wireless sensor networks and Ad-Hoc [1, 4, 5, 17, 18]. But all these approaches ignore the inadequacy observation about the system because some of the experience among the nodes may not be recoded by the system. So there will be uncertainty among the system. And the trust system will have positive trust, negative trust and uncertainty.

In this paper, we used watchdog mechanism to record the experience or observation about its neighbor nodes behavior to build reputation system. Using the binary reputation, and then

we get the trust of its neighbor nodes. In this paper we do not propose how to make a decision for a node whether to cooperate or not to cooperate with its neighbor nodes. We proposed reputation space, trust space and the transformation from reputation space to trust spaces, and some properties about the system for wireless sensor networks. This paper is a basement for further research about reputation and trust system in wireless sensor networks.

3. Modeling certainty

In section 2, we have described some related research work on reputation-based security for wireless sensor networks, S.Ganeriwal, et al [1] use watchdog mechanism to collect data samples and build reputation R_{ij}, and then get the trust $T_{ij} = \frac{\alpha_j + 1}{\alpha_j + \beta_j + 2}$. But the watchdog maybe cannot record all the positive outcomes or negative outcomes for a certain event due to the attacker or fault of the node's hardware. So, we just can sure for a certain event, the watchdog get at least α_j positive outcomes and β_j negative outcomes. The above trust T_{ij} ignores uncertainty. In the following section we will build reputation space, certainty and trust space in wireless sensor networks for reputation-based system

3.1. Watchdog Mechanism

Watchdog scheme can be run on the middleware nodes [1] or on agent nodes [20] in wireless sensor nodes. These nodes use watchdog to monitor the behaviors of nodes within its radio range and functions in a completely distributed manner. In Figure 1, each node holds several modules. Each module carries out a specific function that can classify the collected data and marked as cooperative or uncooperative behavior action.

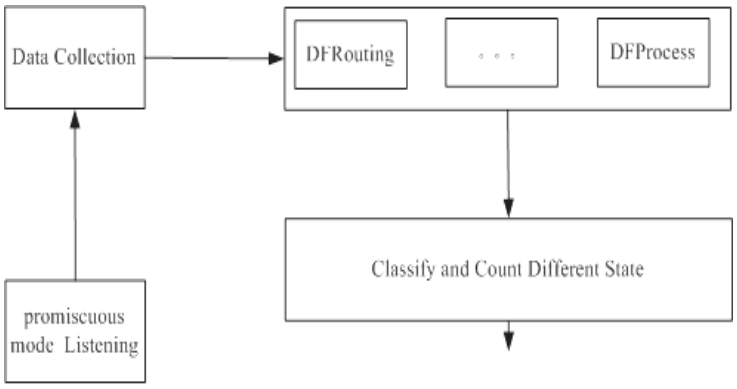


Figure 1. the architecture of Watchdog

The mechanism divided into the following three phases, a) Data collection: the node using a fixed time window function in a promiscuous mode to record behavior of nodes within its radio range. b) Data check: the collected data as input data used in different function module. In figure 1, the watchdog mechanism is consisted by DFRouting and DFProcess modules. DFRouting module monitors the data forwarding behavior of the nodes and checks the behaviors of nodes about routing. DFProcess module monitors the raw sensing data, the data aggregate, the data delay etc. c) State count: according to the result of previous phase, we can classify the behaviors of the nodes into good and bad behavior, and count all the number of

good behavior and bad behavior of each function module, respectively. We call good behavior as positive outcomes and bad behavior as negative outcomes. We use p refer to the numbers of positive; n refer to negative outcomes, respectively. $< p,n >$ is binary event for a certain event of sensor node

3.2. Reputation space

We use watchdog mechanism to gather the first-hand information which we have described in section 3.1. We get p,n , the numbers of positive and negative outcomes, respectively. $< p,n >$ is binary event for a certain event. These numbers would obviously be whole outcomes. However, because the fault of the nodes, attacks or some other reasons, p,n is the at least number of outcomes. Accordingly, we model the reputation space as $RS = N \times N$, a two-dimensional space of integer. The members of RS are pairs $< p,n >$ corresponding to the numbers of positive and negative outcomes in monitor for a special module of watchdog, respectively.

Definition 1: Define reputation space

$$RS = \{< p,n > | \; p,n \in N^{+} \cup \{0\}, t = p + n, \} \tag{1}$$

According to Bayes theorem, $P(B_i \mid A) = \frac{P(B_i)P(A|B_i)}{\sum_{i=1}^{\infty} P(B_i)P(A|B_i)}$ 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].

Definition 2: Define the probability of a positive outcome, x

$$P_{<p,n>}(x) = P(x \mid < p,n >) = \frac{P(<p,n>|x)P(x)}{\sum P(<p,n>|x)P(x)} = \frac{(p+n+1)!}{p!n!} x^{p}(1-x)^{n} \tag{2}$$

S.Ganeriwal, et al [1] probability theory models the event $< p,n >$ by trust, $T = \frac{p+1}{p+n+2}$, which ignore the uncertainty event probability in wireless sensor networks. We will show that if the certainty of event equal to 1, then we get the result as [1].

3.3. Certainty

For motivation, we consider a sensor node A send message to its neighbor node B , and the total number of messages sent to node B was t , some message was received correctly and some message was missed. We supposed exactly p messages was received correctly. So we can get the successful probability that the node A send message to node B is $\frac{p}{t}$ and with certainty $c = 1$. If we have no knowledge about how many total messages were send to node B and how many messages was received correctly, we cannot get the probability and the certainty $c = 0$ .However, if all we known is that at least p messages were received correctly and at least n messages were missed (where $p + n \le t$), then we have partial knowledge. Here $c = \frac{p+n}{t}$. Our key intuition is that using watchdog mechanism, we cannot recorded all the outcomes for a certain event, and the data collected by watchdog are partial knowledge due to the fault of the node or the attacker in wireless sensor networks.

Definition 3: define the certainty based on reputation, $< p,n >$:

$$c(p,n) = \frac{1}{2}\int_0^1 \left| \frac{(p+n+1)!}{p!n!} x^p (1-x)^n - 1 \right| dx \quad (3)$$

Throughout, p, n, and $t = p + n$ refer to positive, negative, and total outcomes, respectively.

3.4. From reputation space to trust space

In wireless sensor networks, using watchdog mechanism, if the watchdog has no any record data about its neighbor node behavior, the trust is $T_{ij} = \frac{1}{2}$ [1]. However, according to our intuition knowledge in our human real world, if one person has no any experience about another person, we cannot get any trust to the person and have no any certainty. So, we have $c = 0$, trust is 0 (positive trust is 0 and negative trust is 0) and uncertainty is 1.

In the following section, we will discuss the transformation from reputation space to trust space, which relates the positive and negative outcomes to positive trust and negative trust, uncertainty. The trust is discount by certainty. And the positive trust is very important for the sensor node to make a decision whether to cooperate. The negative trust is making a criterion to decide a malicious node in wireless sensor networks.

Definition 4: Define trust space:

$$TS = \{(pt, nt, ut)\} \quad (4)$$

where (4) satisfy the following conditions.

$$\begin{cases} pt, nt, ut \geq 0 \\ pt + nt = c \\ pt + nt + ut = 1 \end{cases}$$

In definition 4, pt, nt and ut refer to positive trust, negative trust and uncertainty, respectively. The certainty includes positive trust and negative trust, as in our human real world the trust among people.

Definition 5: Let $T(p,n) = (pt, nt, ut)$ be the transformation from reputation space to trust space, such that $T = (pt(p,n), nt(p,n), ut(p,n))$, where pt, nt and ut satisfy the following conditions:

$$\begin{cases} pt(p,n) = c\frac{p+1}{P+n+2} \\ nt(p,n) = c\frac{n+1}{P+n+2} \\ ut(p,n) = 1 - pt(p,n) - nt(p,n) \end{cases} \quad (5)$$

In definition 5, if certainty equal to 1, then the positive trust becomes $pt(p,n) = \frac{p+1}{p+n+2}$. Importantly, $T = \frac{p+1}{P+n+2}$ is the expected value of the probability of a positive outcome, also characterizes Trust in [1]

4. Properties

In this section, we will discuss some important properties about the relationship among positive outcomes, negative outcomes, total outcomes, positive trust, negative trust and certainty both in reputation space and trust space.

Property 1: If both the positive outcomes and the negative outcomes are 0, then both positive trust and negative trust is 0, the uncertainty is 1.

From our definition 3, we have that if p, n is 0, then $c = 0$. Using definition 5, we can get pt, nt is 0 and ut =1.

As in our human real world, if we have no any knowledge about a certain person, we cannot get any good evaluation or bad evaluation and the probability of uncertainty is 100%.
Property 2: If the ratio $m = \frac{p+1}{p+n+1}$ is fixed, then pt, nt, c are increasing and ut is decreasing when $t = p + n$ total number of outcomes is increasing.

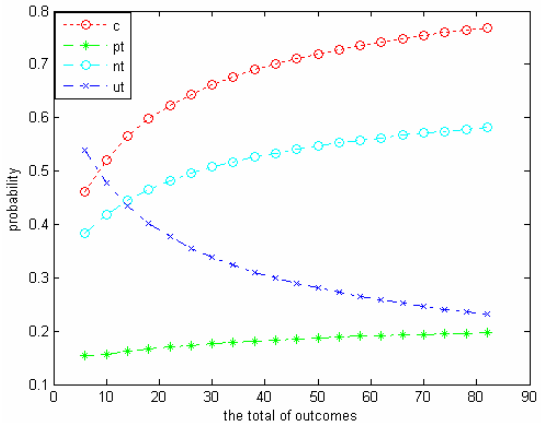


Figure 2 c,pt,nt increase and ut decreases with t when m=0.25 is fixed

Using (3) and $m = \frac{p+1}{p+n+2}$, we have $c(t) = \int_0^1 \left| \frac{(t+1)!}{(mt+2m-1)!(t-mt-2m+1)!} x^{mt+2m-1}(1-x)^{t-mt-2m+1} - 1 \right| dx$ (6)

And the proof ideal is that we can use $c'(t) > 0$ for any $t > 0$.

We can see from figure 2, when the ratio $m = 0.25$ is fixed, the total number of outcomes increases, certainty, positive trust and negative trust increases, but the uncertainty decreases.

In wireless sensor networks, when the watchdog get more data record about a node behavior for a certain event, the node can get more certainty (both positive trust and negative trust) about the node behavior. And then the nodes can get more knowledge to make a decision about the behaviors of the neighbor nodes. We are intuitional get the result in our human real world.
Property 3: when the total outcomes are fixed we have the following property.

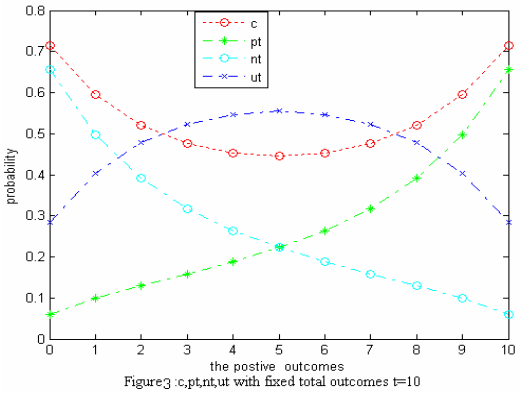


Figure 3 c,pt,nt with fixed total outcomes t=10

1. Positive trust increases and negative trust decreases with positive outcomes increase.
2. The certainty decreases with positive outcomes increase when $p > n$
3. The certainty increases with positive outcomes increase when $p < n$.
4. The certainty reach to the minimum when $p = n$.
5. The uncertainty increase with positive outcomes increase when $p > n$
6. The uncertainty decreases with positive outcomes increase when $p < n$.
7. The uncertainty reach to the maximum when $p = n$

In figure 3, we show the changes of the parameters, c, pt, nt, ut with positive outcomes in fixed total outcomes $t = 10$

Using (3) and $t = p + n$, we have $c(p) = \int_0^1 \left| \frac{(t+1)!}{(p)!(t-p)!} x^p (1-x)^{t-p} - 1 \right| dx$ (7)

And the proof ideal is $c'(p) < 0$ for $2p < t$, $c'(p) > 0$ for $2p > t$, $c'(p) = 0$ for $2p = t$.

From figure 2 and figure 3, we have that positive trust increases with positive outcomes; certainty increases with total outcomes increases.

5. Open Problem

In section 3 and section 4, we have discussed reputation space, trust space and some important properties for reputation-based system in wireless sensor networks. Though lots of research has been done in this field, but there are still in incubation phase for wireless sensor networks and some open problems need to be resolved.

One of the problems is record refresh. In watchdog mechanism, we get the event recodes and then get the reputation $< p, n >$. After a period of time, we will get more record data about an event. How to refresh the reputation value is an issue. If we simple sum all the outcomes about the neighbor, then it is not a well and quickly feedback mechanism. For a sensor node can initially building up a good reputation by being very good behavior and contributive but abuse the system later. It cannot find quickly. Some researcher give different weight to current behavior and the past behavior [1, 4, 5, 6], but all of then is not well done the problem.

Another problem that needs to be addressed is trust data sharing. In reputation system for wireless sensor networks, there are two kinds of import reputation, the first-hand and the second hand. How to converge the first-hand and second-hand reputation is still an import problem.

The third problem is conflicting behavior attack; malicious node can impair good nodes' recommendation trust by performing differently to different nodes. For example, the malicious node i can always behave well to node j and behave badly to another node k. Thus, these two nodes have developed different conflicting opinions about the malicious node i.How to defend this kind attack is still an issue.

Finally, a scheme needs to be developed for a sensor node to make a decision which node is good behavior or misbehavior in wireless sensor networks.

6. Conclusion

Reputation and trust are two very important tools that have been used many field such as economics and e-commerce. But these tools used in wireless sensor networks are still in their incubation phase. In this paper, we have made four important contributions to this work. First, we have presented a reputation space and trust space. Second, we have defined a transformation from reputation space to trust space. Third, we have discussed some important properties about the two spaces. And finally, we point out some open problems in reputation system for wireless sensor networks. With the growing importance of sensor network applications, it helps to provide more accurate reputation-based systems for security in wireless sensor networks.

References

[1]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.
[2]JGeorge Casella and Roger L. Berger. Statistical Inference. Duxbury Press, 1990.
[3]Audun Jsang. "A logic for uncertain probabilities". Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9:279-311, 2001.
[4]S. Buchegger and J.-Y. Le Boudec. “A Robust Reputation System for Peerto-Peer and Mobile Ad-hoc Networks”. Proceedings of P2PEcon 2004, Harvard University, Cambridge MA, U.S.A., June 2004.
[5]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.
[6]A. Srinivasan, J. Teitelbaum and J. Wu. DRBTS: “Distributed Reputationbased Beacon Trust System”. In the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC’06), Indianapolis, USA, 2006.
[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, D. Tygar. “SPINS: Security Protocols for Sensor Networks”. Wireless Networks Journal, September 2002.
[8] F. Ye, H. Luo, S. Lu, L. Zhang. “Statistical Enroute Detection and Filtering of Injected False Data in Sensor Networks”. In Proceedings of IEEE Infocom, 2004.
[9]J. Deng, R. Han and S. Mishra. “The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks”. In the Proceedings of IPSN, April, 2003.
[10] C. Karlof, N. Sastry, D. Wagner. “TinySec: Link Layer Encryption for Tiny Devices”. To appear in ACM SenSys, 2004.
[11]R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, P.Kruus. “TinyPK: Securing Sensor Networks with Public KeyTechnology”. To appear in second workshop on Security in Sensor and Ad-hoc Networks, 2004.
[12]S. Ganeriwal, R. Kumar, C. C. Han. S. Lee, M. B.Srivastava. “Location & Identity based Secure Event Report Generation for Sensor Networks”. NESL Techanical Report, May 2004.
[13]Haiguang Chen, Peng Han ,Bo Yu, Chuanshan Gao “A New Kind of Session Keys Based on Message Scheme for Sensor Networks”. The Seventeenth Asia Pacific Microwave Conference (APMC 2005) Suzhou , China , Dec. 4-7, 2005
[14]A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks”, IEEE Wireless Communications, vol. 11, no. 1, pp. 48-60, Feb 2004.
[15]W. R. Pires, T. H. P. Figueiredo, H. C. Wong,and A. A. F. Loureiro, “Malicious node detection in wireless sensor networks”. in 18th Int’l Parallel and Distributed Processing Symp, 2004.
[16]M. Blaze, J. Feigenbaum, and J. Lacy. “Decentralized Trust Management”. In Proceedings of IEEE Conf. Security and Privacy, Oakland, California, USA,1996.
[17]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.
[18]S. Buchegger and J.-Y. Le Boudec. “Self-policing mobile ad-hoc networks by reputation systems”. IEEE Communications Magazine, July 2005.
[19]Haiguang Chen, Peng Han, Xi Zhou, Chuanshan Gao. Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks. Will be appeared in Pacific Asian Workshop on ISI (PAISI 2007) Chengdu,China, April, 2007.

[20] Haiguang Chen, Huafeng Wu , Xi Zhou, Chuanshan Gao. "Agent-based Trust Model in Wireless Sensor Networks". 8th International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2007)Qingdao, China, July 2007.

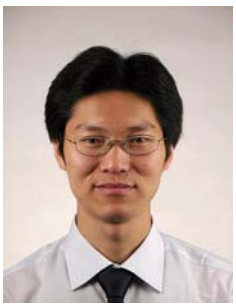
Authors

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.

Gangfeng Gu

is a professor of ShangHai Normal University. His research topic is the application of computer science and distributed networks



Huafeng Wu

is a Ph.D Candidate in the Department of Computer Science and Engineering at the Fudan University, Shanghai, China. His research interests include peer-to-peer networks, sensor networks and ad hoc wireless networks.

Chuanshan Gao

graduated from Fudan University, China, in 1963. Then he worked in the same university. During 1981-1983, he was a visiting scholar in Dept. of CS at UIUC, USA. Now he is director of C & C Lab and professor of Computer Science & Engineering Department at Fudan University. His research interests focus on Data Communication, Computer Networks, Distributed System and their applications. He led and participated in many research projects on the topics mentioned above which have been awarded several times by Province Governments or State Ministries of China. More than 150 papers have been published, most in Chinese and some in English in a well-known international conferences and journals