無線センサーネットワークのための統合トラスト管理機能

郝　東 †　Avishek Adhikari‡　櫻井 幸一 †

† 九州大学大学院システム情報科学学府
{haodong, sakurai}@itslab.csce.kyushu-u.ac.jp

‡ カルカッタ大学純粋数学科
aamath@caluniv.ac.in

あらまし ワイヤレスセンサーネットワークでは、トラストマネージメントが注目されている新たな研究テーマである。しかしながら、完備的なトラストマネージメントシステムを設計した後、完全な安全性を分析することが解決しなければならない問題である。本稿では、クラスタ化センサネットワークに対する新しく完備的なトラストマネージメントメカニズムを提案する。この提案に、ゲーム理論を用いる分析を行い、トラストマネージメントシステムに最適なセキュリティの設定を決定する。まず、中間ノードの行為を観測するため、協力型監視メカニズムを使用する。次に、局部と全局のトラストアルゴリズムを提案する。最後、ナッシュにより、トラストマネージメントシステムの最適なセキュリティ戦略を決定する。

An Integrated Trust Management Mechanism for Wireless Sensor Networks

Dong Hao†　Avishek Adhikari‡　Kouichi Sakurai†

†Graduate School of Information Science and Electrical Engineering, Kyushu University
{haodong, sakurai@itslab.csce.kyushu-u.ac.jp}
‡Department Of Pure Mathematics, University of Calcutta,
aamath@caluniv.ac.in

Abstract Trust management has been recently suggested as one effective security mechanism for distributed systems, and is a promising new approach to solve the security challenges in wireless sensor networks. In this paper, we propose a novel, integrated trust management mechanism for the cluster wireless sensor networks (WSNs), and analyze the optimal decision making policy by using game theory. First, the upstream/downstream joint monitoring scheme is implemented. Then the local trustworthiness and global trustworthiness are derived. Finally, we analyze the interaction between the attacker and the cluster head by using game theory, and define the optimal trust policy based on the analysis result.

1 Introduction

1.1 Background and Related Works

Wireless sensor networks (WSNs) are collections of wireless sensors that are autonomously distributed to gather data from their surrounding environments, to report the changes to data processing center [2]. In WSNs, *trust management* is becoming a new methodology to solve the challenging issues for communication and networks security [1, 2, 3, 4, 5].

The notion trust management is first coined by M. Blaze et al. in [2]. In the literature, many authors address the issues of trust definition in different scenarios for wireless sensor networks. Momani et al. propose the Data trust and Communication trust [6]. Lin et al. introduce Hybrid Trust base on Soft Trust and Hard Trust. These two works take into consideration of the veracity of data, connectivity of path, processing capability of node, and service level of network services. G. Saurabh et al. present a reputation based framework for data integrity for wireless sensor networks. Their scheme considers information which is collected by each insider node running the *Watchdog* mechanism to monitor the neighbors [8]. E. Aivaloglou et al. propose a hybrid trust and reputation management protocol by integrating certificate based trustworthiness and behavior based trust.

1.2 Challenging issues

Based on the special attributes of trust management for wireless sensor networks, and the previous works on this field, the unique challenging issues for establishing the trust management for wireless sensor networks mainly fall into the following categories:

(1) Low Cost Trust Observation and Exchange. In WSNs, if the monitoring scheme is always running, the stringent power will be rapidly consumed. Besides, if the trust information exchange scheme requires too much communication, it will become a burden to QoS [2, 8]. Therefore, light weighted insider behavior monitoring scheme, and efficient insider information exchange scheme are essential for a more effective and low cost trust management mechanism.

(2) Trust Management Mechanism against Insider Threats . The attack by the outsiders may be prevented by crypto-based solutions [8, 9]. However, as the insider attackers are inside the network, and have access to the public/private key systems, they can bypass crypto based secure line [7]. Therefore, to design an effective detecting mechanism, we should implement methods other than cryptographic solutions.

(3) Policy and Decision Making for Trust Management. The final step of trust management is to make a decision about what kind of priority will be authorized to the insider nodes, according to certain decision-making policies. How to make these policies have always been a key problem for trust management, and it deserves a comprehensive theoretical and mathematical analysis.

1.3 Our Contribution

(1) An integrated trust computation and exchange mechanism is implemented. Comparing with previous local reputation based schemes, our integrated trust computation will increase the accuracy and effectiveness of trust computing and exchanging. Moreover, since only the destination nodes need to submit the local trust to the cluster head, this protocol does not require hight communication cost.

(2) We analyze the interaction between the insider attacker and the cluster head as a repeated trust game with mixed-strategy. The final security policy is to classify the insiders into different trust levels. And this policy is defined according to the game equilibrium.

2 Trust Exchange Protocol

2.1 Local Trust Computation

During the time window $TW(t)$, each sender nodes will send several check packets through route x to destination D. In the check packet, for each insider node v_m, there are two categories of opinions: the opinion about packet dropping, and about packet tampering. We first consider the packet dropping. The upstream node v_{m-1}'s opinion on node v_m about packet dropping is defined as:

$$C_F^{up}(v_{m-1}, v_m) = \frac{n_d(v_m)}{n_f(v_m)+n_t(v_m)+n_d(v_m)}$$

where $n_f(v_m)$ denotes the number of packets that node v_m forwards to v_{m+1} and monitored by v_{m-1} by using *Watchdog*; $n_t(v_m)$ denotes the number of packets being tampered by v_m and successfully observed by v_{m-1}, $n_d(v_m)$ denotes the number of packets being dropped by v_m and observed by v_{m-1}.

We then investigate downstream node v_{m+1}'s opinion on v_m about packet dropping, which is denoted as $C_F^{down}(v_{m+1}, v_m)$. In the check packet, the attached number of packets that v_m receive from v_{m-1} is $n_r(v_{m-1}, v_m)$, and the number of packets that v_{m+1} received from v_m is $n_r(v_{m-1}, v_m)$. Then $C_F^{down}(v_{m+1}, v_m)$ can be recorded as:

$$C_F^{down}(v_{m+1}, v_m) = 1 - \frac{n_r(v_m, v_{m+1})}{n_r(v_{m-1}, v_m)}.$$

On receiving the *Check Packet* which contains the opinions C_F^{up} and C_F^{down}, the destination node D will calculate the route x's opinion on each insider node about how they behave on packet dropping:

$$\begin{aligned} C_F(m) = {} & \kappa \times C_F^{up}(v_{m-1}, v_m) \\ & + (1-\kappa) \times C_F^{down}(v_{m+1}, v_m) \end{aligned}$$

κ and $1-\kappa$ are the weights of upstream and downstream nodes' opinion about insider v_m, respectively. Larger $C_F(m)$ indicates v_m drops more data packets between every two check packets.

Besides the opinion about packet forwarding, another item observed is the ratio of packets that have been tampered by the insider v_m, which is denoted as $C_T^{up}(v_m)$. The upstream node v_{m-1} can observe the packet tempering behavior of node v_m by using *Watchdog*. $C_T^{up}(v_m)$ is defined as:

$$C_T^{up}(v_m) = \frac{n_t(v_m)}{n_f(v_m)+n_t(v_m)+n_d(v_m)}$$

After the destination node D receives the check packet, it will generate $C_T(m)$ to denote the route x's opinion on insider v_m about packet tampering. Note that $C_T(m) = C_T^{up}(v_m)$. The local trust value from route x for an insider node m is denoted as T_{xm}^{local}, which consists of two parts, one is trust for packet tampering and the other one is trust for packet dropping:

$$\begin{cases} T_{xm}^{local}(T) = \sum\limits_{i}^{N_{cp}^{x}} RT_{xm}(i) \times \mu1_{cp}/N_{cp}^{x} \\ T_{xm}^{local}(D) = \sum\limits_{i}^{N_{cp}^{x}} RD_{xm}(i) \times \mu2_{cp}/N_{cp}^{x} \end{cases}$$

where $RD_{xm}(i)$ (or $RT_{xm}(i)$) is the value of $C_F(m)$ (or $C_T(m)$) corresponding to the i-th check packet, $\mu1_{cp}$ and $\mu2_{cp}$ are the discount factors of trustworthiness which mean the decaying of trust over time. N_{cp}^{x} denotes the total number of check packets generated along route x during time window $TW(t)$.

2.2 Global Trust Computation

Let Ω denote the set of all the N routes which contain the insider m in the window $TW(t)$, and $x \in \Omega$ be one route. Let $H(x, m, t)$ denote how many times that insider m has forwarded packets for route x during $TW(t)$. Therefore, the total number of times that insider m has been used in $TW(t)$ is recorded as $H(m,t) = \sum_{x\in\Omega} H(x,m,t)$. Let $T_{xm}^{local}(i) \in [0,1]$ denote the local trustworthiness of insider m towards the view on the route x, where i can be $Packet\_Tamper$ or $Packet\_Drop$. After these, the global trust value can be defined as a function of $T_{xm}^{local}(i)$ and $H(x,m,t)$:

$$T_m(i) = \sum_{x\in\Omega} \left[\frac{H(x,m,t)}{\sum_{x\in\Omega} H(x,m,t)} \times T_{xm}^{local}(i) \right]$$

where $i \in \{T, D\}$. The value of the global trust measures a generalized trustworthiness of an insider m in the view of all routes, during the last time window $TW(t)$. Based on this global trust values during the past $TW(t)$, the cluster head will classify the insider nodes into different categories (e.g., *Legitimate*, *Suspicious* or *Malicious*).

3 Trust Game Model

In the last section, the global trust value is derived. Based on this global trust value of each insider nodes, the cluster head need to make a security decision. This decision should be on the foundation of security analysis. In this section, we analysis the interaction between the attacker and the cluster head, and define the security policies for the WSNs. In clustered WSNs, the game is between any one of the insider attackers who takes attack strategies, and the cluster head who makes decision on how to classify the insiders based on the global trust values. The attacker wants to bring damage to the network, and the cluster head wants to prosecute the attacker out. The loss of the network system is the same as the gain of the attacker. Therefore, we model the game as zero-sum non-cooperative game [11].

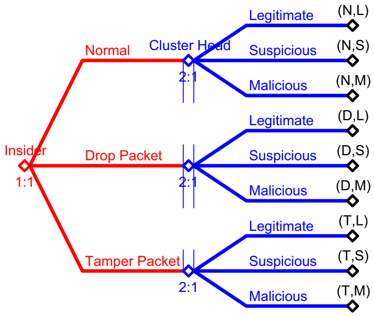

図 1: Extensive Form of Trust Game

3.1 Trust Game Construction

Fig.1 portrays the one-shot trust game between the insider and the cluster head. This game is illustrated as a tree in which the attacker takes its attack strategy first and the cluster head takes the defense strategy in succession after the attacker. The red node at the root denotes the insider, and 1:1 means the first move of the first insider node. The insider node may take any one of the 3 strategies: *Behave Normally* (N), *Drop Packet* (D), and *Tamper Packet* (T), which are presented by red lines starting from the root. Similarly, the cluster head's moves start from a blue node, and 2:1 means the first move of the cluster head. The cluster head can make 3 kinds of decisions: Trust the insider, classify it as *Legitimate* (L), Semi-Trust the insider, consider it as *Suspicious* (S), and completely distrust the insider, classify it as *Malicious*(M).

3.2 Trust Game Outcomes

In the game tree illustrated in Fig.1, we can see that, the attacker first choose its attack strategy (red lines), then the cluster head choose the defense strategy (blue lines). At the end of the game tree (leaf nodes), the game will come to nine possible outcomes. At each different outcome, both the attacker and the defender may receive a reward. The outcomes of this game are: (N, L):

Insider node behaves normally, and cluster head trusts the insider, classify it into legitimate member; (N, S): Insider node behaves normally, but cluster head mistakenly semi-trusts it, and classifies it as suspicious insider; (N, M): Insider node behaves normally, while cluster head makes an error, distrusts it, and classifies it as malicious attacker; (D, L): Insider node drops packets, but cluster head considers the drop as due to channel problems, classifies the insider as Legitimate Member; (D, S): Insider node drops packets, and cluster head correctly semi-trusts it, classifies it as suspicious and requires further observation; (D, M): Insider node drops packets, and cluster head distrusts it, severely classifies it as malicious and isolates it from service; (T, L): Insider node tampers some packets, but cluster head makes an error, wrongly trusts it, and regards it as legitimate; (T, S): Insider node tampers some packets, while cluster head classifies it as suspicious and requires further observation; (T, M): Insider node tampers some packets, and cluster head regards it as malicious and isolates it from service;

The corresponding payoff for the insider at each of the outcomes is denoted as $U_m(u, v)$, where $u \in \{N, D, T\}$ is the strategy from insider, and $v \in \{L, S, M\}$ is the strategy from the cluster head. Since in the network, the attacker's gain is the the network's loss, therefore the utility of the network is $U_n(u, v) = -U_m(u, v)$, which indicates a zero-sum game [12]. We illustrate the utilities as the matrix in Table.1, in which the $U_n(u, v)$ may vary in different application scenarios [8].

4 Trust Game Equilibrium

The key point in the game analysis is the Nash equilibrium. We explore the Nash equilibrium points, the outcome in which neither the insider nor the cluster head wants to unilaterally change its strategy. Otherwise, the change will only lead to its own utility degradation[11, 12]. In the field of network security and trust management, a security analysis deserving its name is a min-max method that the defender first looks at the maximal damage that an attacker can cause for a specific defence, and then searches for the defence that minimizes the maximal damages[5, 12]. This min-max decision rule, in zero-sum game theory, is well known as the necessary and sufficient condition for the Nash equilibrium[11].

We utilize the min-max rule to approach the Nash equilibrium. Taking into consideration the payoff matrix in Table 1 and the Joint distribution of mixed-strategy matrix in Table 2, the trust game's Nash equilibrium $(s_m^*(p, q), s_n^*(x, y))$ is restricted to the following function set:

$$\begin{cases} s_m^*(p, q) = \arg \min\limits_{s_m(p,q)} \max\limits_{s_n(x,y)} \mathbb{E}_m \left(s_n(x, y), s_m(p, q)\right); \\ s_n^*(x, y) = \arg \max\limits_{s_n(x,y)} \min\limits_{s_m(p,q)} \mathbb{E}_m \left(s_n(x, y), s_m(p, q)\right). \end{cases}$$

where $s_m(p, q)$ and $s_n(x, y)$ are the mixed strategy of attacker and cluster head, respectively. Furthermore, $s_n^*(x, y)$ denotes the dominant mixed strategy in which the value of x and y will bring the network with the optimal utility. $s_m^*(p, q)$ denotes the optimal mixed strategy of the attackers. Considering utilitys at each outcome, $\mathbb{E}_m \left(s_n(x, y), s_m(p, q)\right)$ is the *overall utility expectation* in the status that attacker chooses the mixed strategy $s_m(p, q)$ while cluster head chooses the mixed strategy $s_n(x, y)$. This utility expectation is calculated by the mathematical expectation over the utility matrix from Table 1, taking into consideration of the mixed strategies in Table 2.

According to [11], every finite strategy game has at least one mixed strategy Nash equilibrium. Given the real numbers of the elements in Table 1, the above min-max function can be easily solved by nonlinear optimization method. Then the values of p, q, x and y can be derived. The values of p, q, and $1 - p - q$ are the thresholds for the global trust values $T_m(i)$ according to equation (6). Comparing with the thresholds p, q and $1 - p - q$, if $T_m(Packet\_Tamper)$ is higher than $(1 - p - q)$, the insider m should be considered as malicious; if $T_m(Packet\_Drop)$ is higher than q, the insider m should be at least viewed as suspicious. As the time window $TW(t)$ changes, the strategies of both the attacker and the cluster head will also change, this is about the evolution of the trust game, which will be discuss in the next subsection.

5 Trust Game Evolution

Since the communication of the network goes on, there are multiple time windows, the trust game is extended to multi-stage repeated game. We utilize the Quantal Response Equilibrium (QRE)[10] which is a generalization form of multi-round game Nash equilibrium to analyze the evolution of this trust game. The QRE is calculated by the following equation:

$$P_i^k = \frac{\exp(\lambda \times EU_i^k(P_{-i}))}{\sum_m \exp(\lambda \times EU_i^m(P_{-i}))}$$

where P_i^k is the probability for player choosing strategy k, For the attacker, P_i^k can be p, q or $1 - p - q$. While for the defender, P_i^k can be x, y

表 1: Different Payoffs for Network at Different Outcomes

Strategy	*Trust*	*Semi-Trust*	*Distrust*
Behave Normally	$U_n(N,L)$	$U_n(N,S)$	$U_n(N,M)$
Drop Packets	$U_n(D,L)$	$U_n(D,S)$	$U_n(D,M)$
Tamper Packets	$U_n(T,L)$	$U_n(T,S)$	$U_n(T,M)$

表 2: Different Payoffs for Network at Different Outcomes

Strategy	*Trust*	*Semi-Trust*	*Distrust*
Behave Normally	px	py	$p(1-x-y)$
Drop Packets	qx	qy	$q(1-x-y)$
Tamper Packets	$(1-p-q)x$	$(1-p-q)y$	$(1-p-q)(1-x-y)$

or $1-x-y$). $EU_i^k(P_{-i})$ is the expected utility to player i of choosing strategy k given other players are playing according to the probability distribution P_{-i}. In the trust game, $EU_i^k(P_{-i})$ is equal to $U_n(i,j)$. Larger λ indicates that the players become *more rational*, and are more eager to take Nash equilibrium strategies.

We consider two kinds of attackers: *1)Smart insider attackers* who are rational, prefer to protect itself, hide in the network and launch long-term attack; *2)Naive insider attackers*, who are irrational, and want to launch severe attacks even taking the risk of being detected. Following the utility preference ordering method [13], the smart attacker's preference sequence of all the potential 9 outcomes is: $(T,L) > (D,L) > (T,S) > (D,S) \simeq (N,L) \simeq (T,M) > (N,S) > (D,M) > (N,M)$. On the contrary, the naive attackers will give more importance in bringing damage to the wireless network systems, than protect themselves. Therefore, its preference sequence for the potential outcomes is: $(T,L) > (T,S) > (D,L) > (D,S) \simeq (N,L) \simeq (T,M) > (D,M) > (N,S) > (N,M)$. Also following the method in [13], the example utilities $U_n(i,j)$ are defined. Then by using the tool GameBit [14], the QRE of the repeated trust game is derived.

In Fig.2 the red lines indicate the evolution of the strategies of naive attacker. The repeated trust game starts with equal probabilities (0.33) for each strategy. With the increase of $TW(t)$, the trust game also repeats. In Fig.2(a), the naive attacker's probability for normal behavior (N) decreases faster than the smart attacker. In Fig.2(c), the smart attacker slowly increases its probability for tampering packet, to avoid being detected, while the naive attacker have less fear of taking risks, and is more eager to tamper packets. From this, we are aware of that the smart attacker are more tricky to avoid being detected. Any insider whose strategy trajectories locate on the left of the red lines, should be classified as malicious immediately; Any nodes whose trajectories is on the right of the blue lines, can be considered as legitimate temporarily; And those nodes whose strategy evolution trajectory between the red and blue lines, should be at least viewed as suspicious.

6 Conclusion

We proposed an integrated trust management mechanism for clustered wireless sensor network. The behavior of insider nodes are observed by a light weight upstream/downstream joint monitoring scheme. The opinions from the monitors are then calculated to get the local trust value. Local trust values are then submitted to the cluster head, and the global trust is generated according to our trust calculation and exchange algorithm. After that, the threshold for the global trust, is analyzed by a mixed-strategy repeated trust game. The analysis not only considers static case in which the trust game only runs one-shot, but also extends the attacker-defender trust game to a repeated scenario. The optimal trust policy is made based on the mixed strategy game analysis. By using this trust management mechanism, it is possible for the WSNs to reduce the potential damage from the

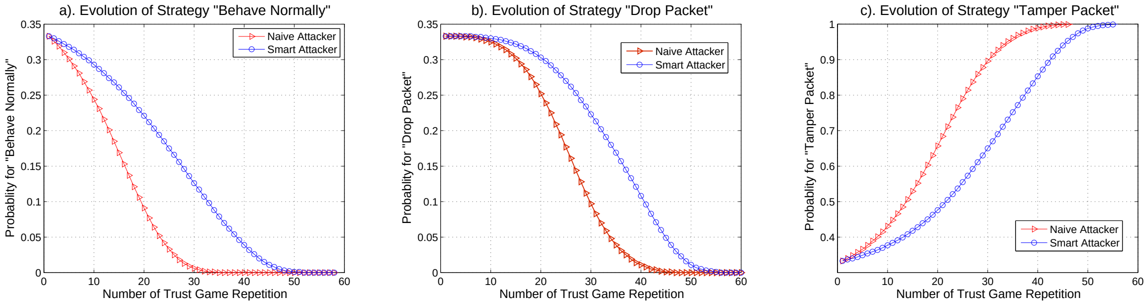

図 2: Comparison of Strategy Evolution of the Smart and Naive Attackers

malicious and suspicious insider attacker to minimum. Our future work is to implement this trust management mechanism, and design an effective intrusion detection system for WSNs.

Acknowledgments

The first author Dong HAO and the last author Prof. Kouichi SAKURAI's research is partly supported by Grants-in-Aid for Scientific Research (B) (23300027), Japan Society for the Promotion of Science (JSPS). Dong HAO is a Ph.D candidate at Kyushu University and he is supported by the governmental scholarship from China Scholarship Council. The second author Dr. Avishek Adhikari is (partially) supported by JAPAN SCIECE AND TECHNOLOGY AGENCY (JST), Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields, entitled "Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science."

参考文献

[1] A. Perrig, J. Stankovic, D. Wagner. "Security in wireless sensor networks." Commun. ACM 47, 6 June 2004. pp. 53-57.

[2] M. Blaze, J. Feigenbaum, and J. Lacy. "Decentralized trust management." In Proc. of IEEE SRSP, May. 1996. pp. 164-173.

[3] A. Josang, R. Ismail, and C. Boyd; "A survey of trust and reputation systems for online service provision." March 2007. pp. 618-644.

[4] A. Josang, R. Hayward, and S. Pope; "Trust network analysis with subjective logic." 29th Australasian Com. Sci. Conf. pp. 85-94.

[5] D. Gollmann; "From Access Control to Trust Management, and Back - A Petition"; IFIPTM2011, Copehagen, Denmark. pp. 1-8.

[6] M. Momani, S. Challa, R. Alhmouz; "Can we trust trusted nodes in wireless sensor networks?" ICCCE 2008. pp. 13-15.

[7] D.M. Shila, Y. Cheng; "Mitigating selective forwarding attacks with a Channel Aware Approach in WMNs" IEEE Transaction on Wireless Communications, May, 2010. pp. 1661 - 1675.

[8] F. Anjum, P. Mouchtaris. Security for Wireless Ad Hoc Networks, Wiley. 2007.

[9] R. G. Bace, Intrusion detection, Macmillan Publishing Co., Inc. 2001.

[10] M.K. Richard; P., Thomas, "Quantal Response Equilibria for Extensive Form Games"; Experimental Economics, 1998. pp. 9-41.

[11] R. Gibbons.; Game Theory for Applied Economics.; Princeton University Press. Princeton. NJ. 1992.

[12] T. Alpcan, T. Basar. Network Security: A Decision and Game Theoretic Approach. Cambridge University Press. 2010.

[13] K. Binmore; Playing for real: a text on game theory; Oxford University Press, 2007.

[14] M. Richard D., M.L., M. Andrew, and T.L. Turocy, (2010). Gambit: Software Tools for Game Theory, http://www.gambit-project.org.