Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks

Dong Hao[1], Avishek Adhikari[2], and Kouichi Sakurai[1]

[1] Graduate School of Informatics, Kyushu University, Japan
haodongpost@gmail.com, sakurai@csce.kyushu-u.ac.jp
[2] Department of Pure Mathematics, University of Calcutta, India
aamath@caluniv.ac.in

Abstract. Wireless sensor networks are vulnerable to a large number of security threats and malicious attacks. The traditional security approaches from encryption and authentication are insufficient to defend the insider attacks which are launched inside of the WSNs and bypass the crypto-based defence. Trust management has been recently suggested as one of the effective security mechanisms for distributed systems, and is a promising new approach to solve the security challenges in wireless sensor networks. However, to the best of our knowledge, it is still a challenge to establish an integrated trust management mechanism with comprehensive security analysis. In this paper, we consider the clustered wireless sensor network in which the cluster head is in charge of the trust management of other sensor nodes. We propose a novel, integrated trust management mechanism for the cluster wireless sensor networks, and analyze the optimal decision making policy by using game theory. First, the upstream/downstream joint monitoring scheme is implemented to securely and efficiently observe the behavior of the insider nodes. Then based on the monitoring results, the local trustworthiness and global trust worthiness are derived based on the trust exchange and the trust computation. Finally, by game theoretic analysis of the security interaction between the attacker and the network, the optimal trust policy can be made based on min-max rule, and the optimal utility of the WSNs can be guaranteed.

Keywords: Clustered Wireless Sensor Networks, Trust Management, Insider Threats, Mixed-Strategy Game, Quantal Response Equilibrium.

1 Introduction

1.1 Background and Related Works

Wireless sensors are small and inexpensive devices powered with low-energy batteries, equipped with radio transceivers, and capable of responding to physical radio signals. 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[1]. Though the

L. Chen, M. Yung, and L. Zhu (Eds.): INTRUST 2011, LNCS 7222, pp. 239–257, 2012.

development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and civilian applications[1, 20].

Although wireless sensor network is promising for various important applications, the security issues in wireless sensor networks have been a roadblock for their development[2, 20]. The critical goal of networks is to protect the network against various attacks which is especially putting more threat to wireless sensor networks due to their characteristics such as open medium, multi-hop, and dynamic topology[1, 20, 21]. The attacks against wireless sensor networks mainly fall into two categories: (1) Outsider attack: The adversary adopts the methods including eavesdropping on information, injecting fractional data to jam the networks traffics, and fabricating fake records to disturb the normal function of the network[20, 21]. For these kinds of outsider attacks, it is of no necessary for the adversary to compromise any insider sensor nodes thoroughly. (2) Insider attack: The adversary breaks through the safeguard (e.g. the cryptographic and authentication mechanisms), and consequently, the insider nodes are compromised by the adversary and are changed into malicious attackers[18–20, 30, 35]. Traditional security systems are mainly used to protect the WSNs from outsider attacks. However, since the insider attackers have access to the public and private keys and bypass the cryptography system, it is preferred to use cryptographic solutions as a first line of defence, and utilize non-cryptographic solutions as a second line to protect the network against the insider attackers[14].

In contrast to the conventional approaches, *trust management* is becoming a new methodology to solve the challenging issues for communication and networks security [2–13, 17, 22, 24, 28]. The notion trust management is first coined by M. Blaze et.al in 1996[3]. The original trust management is about making the policy for the authorization to strangers, by means of recommendations from third parties. Trust management is then embodied as a distributed authentication system. Several later access control systems such as SPKI (simple public key infrastructure)[15] and dRBAC(distributed role-based access control)[16] are also inspired by the idea of trust management. With the advancement of the research, the subsequential studies of trust management have approached to the extensive fields as evaluation, analysis, and quantification of the trust and trustworthiness of network entities over time. The key problem towards the studies of trust management is to obtain the precise, practicable trust values and correspondingly, how to make the optimal trust policies[6].

Similar to the implementation of trust management in wired networks[5], online service, and e-commerce systems[4], it is also of significance to introduce the trust management into the fields such as ad hoc networks, peer-to-peer networks, and also wireless sensor networks. Since the insiders are capable to launch attacks and break the crypto-based security systems, trust management is considered as one effective second line of defence for the wireless network security[7–12, 14, 17, 18, 32]. As a natural consequence of introducing trust management into wireless sensor network environments, trust has been put forward with quite different meanings and corresponding features. In wireless sensor networks, taking into consideration of trust management, each sensor node is assigned a trust value to reflect its trustworthiness according to its historical behavior and performance. And trustworthiness in WSNs is generally interpreted as belief, subjective probability and reputation which represent the quantified values of availability, realisability, or security property of the insider nodes. Obtaining the behavior record of the insider nodes of WSNs, the trust management scheme then calculate the trust value and carry out reward or punishment according to the specific trust policies[6].

In the literature, many authors address the issues of trust definition in different scenarios for wireless sensor networks[7–12]. Momani et al. propose the Data/Communication trust[9]. 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[7]. R.A. Shaikh et al. introduce peer evalutaion scheme based on direct observation of the monitor and recommendations from a third node. Therefore their work is based on group trust[8]. E. Aivaloglou et al. propose a hybrid trust and reputation management protocol by integrating certificate based trustworthiness and behavior based trustworthiness[11].

1.2 Challenging Issues

As discussed above, being an alternative solution to traditional security mechanisms, trust is gradually utilized in wireless sensor networks security[9], to maintain and manage the historical behavior of the insiders (generally known as *reputation*), and make policies for authorization or feedback (reward or punishment) to these insiders. In a word, trust for wireless sensor networks, is a mechanism that deals with the insider threats, based on historical behavior observations and decision policies[6]. A typical trust mechanism for WSNs should contain these important components.

- *Monitoring scheme*, which is preferred to be light weighted.
- *Trust information exchange*, which is required to be low cost.
- *Trust Policies* for authorization or reward/punishement decision.

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. Existing trust management mechanisms are mostly used in wired distributed systems, which differ from the WSNs trust management application, especially in the aspects of power-consumption and performance observation model. Therefore, it is of great significance to reconstruct these existing schemes to make them acclimate to the new

WSNs environments. Concretely, in WSNs, if the monitoring scheme is always running, the stringent power will be rapidly consumed[30]. Besides, if the trust information exchange scheme requires too much communication, it will become a burden to QoS[1, 20, 24]. 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 against Insider Threats. The outsider attacks may be prevented by crypto-based solutions[20, 21]. However, as the insider attackers are inside the network, and have access to the pubilic/private key systems, they can bypass such secure systems[14]. Therefore, to design an effective detecting mechanism, we should implement methods other than cryptographic solutions as the alternative solution to cryptography. At the same time, we should also take into consideration the stringent power resource of each monitoring node.

(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. This kind of policy should guarantee that the network will maximize its potential utility, in other words, reduce the attacker's damage to minimum[6]. Thus, 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

In view of the above related works and the challenging issues, in this paper, we propose an integrated trust management mechanism for the wireless sensor networks. We consider the clustered wireless sensor networks in which at least one cluster head exists among the insider nodes. The main objective of our trust management mechanism is to observe the historical behavior of insider nodes, exchange the observations from different routes, and make security decisions for classifying different insider nodes into different trustworthiness level, according to the trust policies.The main contributions of our work are summarized as:

(1) To observe the behavior of insider nodes, and to collect the evidence for trust management, we implement a light weight upstream/downstream joint monitoring scheme. By using this scheme, each insider will be observed by its upstream and downstream neighbors. By utilizing *Watchdog* and signed *Check Packets*, this joint monitoring scheme can be made cheat-proof. As well, the joint monitoring can reduce power consumption comparing to previous monitoring schemes which require either complex computation or need to be run in the *promiscuous mode*[20] consistently.

(2) An integrated trust computation and exchange mechanism is implemented. By using the check packet, each insider node will send its opinion on both its upstream and downstream neighbors to the destination node. Then destination node for each route will calculate the *local trust* of the insiders based on the information from the check packet, and then submit the local trust values to the

cluster head. The cluster head, which is capable of calculating the global trust, will finally make an authorization decision, and inform the decision to all the inside nodes in this network. 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.

(3) 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. This trust policy will bring the network system with optimized utility, by choosing the defence strategies that minimize the attack damages which the attacker wants to maximize. Without loss of generality, we consider two kinds of attackers: smart attacker and naive attacker, and we reveal the security decision making should be different for these two kinds of attackers.

2 Upstream and Downstream Joint Observation

One important issue to detect the misbehaving insiders in WSNs is how to identify the misbehavior, including packet dropping and packet tampering. In this section, we utilize the upstream/downstream monitor scheme[14] to maintain the history of packet loss and tamper at an arbitrary insider node.

2.1 Insider Threat Scenario

In WSNs, the insiders are the sensor nodes which have legitimately registered into the network and have legal identities and access to the public/private key system. The insider attacks in WSNs focus on the users which had internal access to information and network systems[18, 19, 34].

Following the reactive routing protocols[20], when a source node S wishes to send its data packets to the destination node D, it will first broadcast its Route Request message[1, 3, 20]. On receiving this message, the insiders which have the existing route to D will reply a Route Response message, and sender will include the insiders which have good behavior history into its route to the destination D. After that, sender S will begin to transfer its data packets to destination D. On receiving the data packets from S, each insider can decide either to forward these packets or to drop them, or to tamper the packets. If the packets are dropped by the insiders, the packet receive ratio at D will decrease and the network performance will drop dramatically which reflects that the integrity is damaged. If the packets are tampered by the insiders, the confidentiality and availability will be damaged. Since packet tampering is more difficult to be detected, we consider that it causes more damage to the network than packet dropping.

2.2 Joint Monitoring in One Route

The whole network communication is divided into multiple *time windows*. In each segment of these time windows $TW(t)$[20], there are many routes responsible for data packet forwarding. To perceive the misbehavior of the WSN insiders, the most direct way is *traffic monitoring*[1, 20, 21]. Utilizing the upstream/downstream joint monitoring scheme[14], each node can be observed by its upstream and downstream neighbors in the route.

Consider in route x, the sender sends its data packets through the insider nodes $v_1, v_2, ..., v_m, ..., v_n$. Each time an insider v_m receives a data packet, it will update its local counter about how many packet it has received from its upstream neighbor v_{m-1}. We record this number as $n_r(v_{m-1}, v_m)$. Then the insider v_m will forward the data packet to its downstream neighbor v_{m+1}. Working under the *Promiscuous Mode*[20], sensor nodes are capable of observing the downstream nodes within its broadcast domain, about whether it tamper, drop or forward the packets, respectively. The node v_m will record the number of packets v_{m+1} dropped as $n_f(v_{m+1})$, the number of packets v_{m+1} tampered as $n_t(v_{m+1})$, and the number of packets v_{m+1} dropped as $n_d(v_{m+1})$.

Let $M_{S\to D}$ be an integral number. To obtain the trust of all the insider nodes along the route x, after every $M_{S\to D}$ data packets, the sender S will generate a *check packet*, and send it thought the route x to destination node D. When this check packet passes through route x, each insider in x will attach its opinions about its upstream and downstream neighbors to the variable field in the check packet. Noting that within one time window $TW(t)$, along one route x, there may be multiple check packets.

Consider a simple but representative case, when the insider m is included in a 5-hop route, described as $S \rightleftharpoons v_1 \rightleftharpoons v_2 \rightleftharpoons v_3 \rightleftharpoons D$, where S and D denote the sender and destination node, respectively. When the check packet passes each node, the node will attach their messages to the the empty fields in the check packet. The information in the check packets along the 5-hop route is:

$$
\begin{aligned}
&S \overset{M_0}{\to} v_1 : M_0 = S \,\|M_{S\to D} \,\|C_F^{up}(S, v_1), C_T^{up}(v_1) \,\|Sign(S);\\
&v_1 \overset{M_1}{\to} v_2 : M_1 = M_0 \,\|v_1 \,\|n_r(S, v_1) \,\|C_F^{down}(v_1, S) \,\|C_F^{up}(v_1, v_2), C_T^{up}(v_2) \,\|Sign(v_1);\\
&v_2 \overset{M_2}{\to} v_3 : M_2 = M_1 \,\|v_2 \,\|n_r(v_1, v_2) \,\|C_F^{down}(v_2, v_1) \,\|C_F^{up}(v_2, v_3), C_T^{up}(v_3) \,\|Sign(v_2);\\
&v_3 \overset{M_3}{\to} D : M_3 = M_2 \,\|v_3 \,\|n_r(v_2, v_3) \,\|C_F^{down}(v_3, v_2) \,\|C_F^{up}(v_3, D) \,\|Sign(v_3).
\end{aligned}
$$

The message attached to the check packet at each node are denoted as M_0, M_1, M_2 and M_3, respectively. The first field in M_0 and second field in M_1, M_2 and M_3 are the identities of each node. $M_{S\to D}$ is the total number of data packets S has sent to D during between every two check packet. C_F^{up} is the upstream neighbor's opinion on how the insider node behaves on packet dropping, based on the *Promiscuous mode* monitoring such as *Watchdog*. It describes the percentage of packets that an insider node drops, and observed by its upstream neighbor. For instance, $C_F^{up}(S, v_1)$ is S's opinion on insider v_1 about how v_1 behaves as packet dropping. On the other hand, C_F^{down} is downstream neighbor's opinion on how the insider node behaves as packet dropping, which also indicates the percentage of packets that an insider node m drops. C_T^{up} is the upstream neighbor's opinion on how one insider behaves as packet tampering. Finally, at each node, the message is attached with an Elliptic Curve Digital Signature $Sign(v_m)$[20]. The signature is generated based on the node's identity v_m, and can protect this message from being tampered.

On receiving the check packet, the destination node will retrieve the ID of each insider node, and verify the signatures. After that, the destination node will calculate the local trust of each insider node m in this route, based on the m' upstream/downstream neighbors' opinions. In the next section, we will introduce the local trust and global trust computation and exchange.

3 Trustworthiness Exchange Protocol

In the last section, the upstream/downstream joint monitoring scheme is implemented, and the insiders' historical behavior can be obtained by such monitoring scheme. Based on the observation records, in this section, we propose the local trust computation and global trust exchange protocol. The local trust means the trust values that are generated based on the monitoring information from a single route, while the global trust is the integrated trust value which collects the opinions on one insider node from all the routes.

3.1 Local Trust Computation

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. As we illustrated in the last section, the upstream node v_{m-1}'s opinion on node v_m about its packet dropping is recorded as $C_F^{up}(v_{m-1}, v_m)$, which is located between interval $[0, 1]$. By using *Watchdog*[20] mechanism, the upstream node v_{m-1} can overhear whether node v_m forwards, drops, or tamper packets. Then $C_F^{up}(v_{m-1}, v_m)$ can be calculated as:

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

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}. And $n_d(v_m)$ 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 $C_F^{down}(v_{m+1}, v_m)$. This opinion is generated according to the number of packets each node received, which is attached in the check packet, and it is also a real number located between interval $[0, 1]$. Recall that, in the check packet, the attached number of packets that v_m receives 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 node $C_F^{down}(v_{m+1}, v_m)$ can be recorded as:

$$C_F^{down}(v_{m+1}, v_m) = 1 - \frac{n_r(v_m, v_{m+1})}{n_r(v_{m-1}, v_m)} \tag{2}$$

On receiving the *Check Packet* which contains the opinions $C_F^{up}(v_{m-1}, v_m)$ and $C_F^{down}(v_{m+1}, v_m)$, the destination node D will calculate the route x's opinion on each insider node about how they behaves as packet dropping:

$$C_F(m) = \kappa \times C_F^{up}(v_{m-1}, v_m) + (1 - \kappa) \times C_F^{down}(v_{m+1}, v_m) \tag{3}$$

Since the accuracy of upstream monitoring and accuracy of downstream monitoring are different, we define κ and $1 - \kappa$ as the weights of upstream and downstream nodes' opinion about insider 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:

$$C_T^{up}(v_m) = \frac{n_t(v_m)}{n_f(v_m) + n_t(v_m) + n_d(v_m)} \tag{4}$$

where $n_f(v_m)$, $n_t(v_m)$ and $n_d(v_m)$ have the same meanings as in equation (1). 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. And $C_T(m) = C_T^{up}(v_m)$.

After the destination node D generates $C_F(m)$ and $C_T(m)$ for all the insiders in its route x, it will calculate the local trust value of the insiders in route x. 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:

$$\begin{cases} T_{xm}^{local}(Packet\_Tamper) = \sum_{i}^{N_{cp}^x} RT_{xm}(i) \times \mu 1_{cp} / N_{cp}^x \\ T_{xm}^{local}(Packet\_Drop) = \sum_{i}^{N_{cp}^x} RD_{xm}(i) \times \mu 2_{cp} / N_{cp}^x \end{cases} \tag{5}$$

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. $\mu 1_{cp}$ and $\mu 2_{cp}$ 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 $TW(t)$.

The metrics $T_{xm}^{local}(Packet\_Tamper)$ and $T_{xm}^{local}(Packet\_Drop)$ are called *local trust* for the reason that it indicates only the route x's opinion on insider node m. However, local trusts are insufficient to evaluate the insiders' trustworthiness. First, if only local trust is conducted, it will take a long time for a node to obtain enough observation records of all the other nodes in the network. Second, one insider may behave maliciously in one route, but legitimately in another route.

This may mislead those routes that have not been attacked before. Therefore, a comprehensive global trust value which is integrated from all the local routes is required.

3.2 Global Trust Computation

Assume within time window $TW(t)$, there are N routes along which the insider node m participates in. In other words, those N routes intersect at node m. At the end of $TW(t)$, the destination nodes of each route will submit the local trust value on the insiders to the cluster head. It is assumed that the cluster head is the trusted third party (TTP). Because if the cluster head is compromised by adversary, the entire network will also be besieged soon.

Let Ω denote the set of all the N routes which utilized insider m in the window $TW(t)$, and $x \in \Omega$ be one route. Let $H(x, m, t)$ be the number of times that route x has utilized the insider m during $TW(t)$. Therefore, the total number of times that insider m has been used in the past time window $TW(t)$ 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 in the view of route x, where $i \in \{Packet\_Tamper, Packet\_Drop\}$. And let $Kr(x, t)$ be the balance factor of trust value from route x, during time window $TW(t)$. $Kr(x, t)$ is introduced to offset the risk of non-credible feedbacks from route x, such as bad-mouthing attack or whitewashing attack[20]. After these, the global trust value can be defined as a function of $T_{xm}^{local}(i)$, $H(x, m, t)$, and $Kr(x, t)$:

$$T_m(i) = \sum\nolimits_{x\in\Omega} \left[\frac{H(x,m,t)}{\sum_{x\in\Omega} H(x,m,t)} \times T_{xm}^{local}(i) \times Kr(x, TW(t)) \right] \tag{6}$$

where $i \in \{Packet\_Tamper, Packet\_Drop\}$. The value of global trust measures a generalized trustworthiness that an insider m is held by all the routes, which utilized m as an insider node 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* and *Malicious*). The legitimate insiders will be permitted to access more services of the network system. The malicious insiders will be isolated from the system immediately. And for the suspicious insiders, the cluster head will inform all the member nodes that such suspicious insider should be given more frequent observations. For example, each route x may reduce the value of $M_{S\to D}$ which will increase the frequency of generating the *check packet* to check the suspicious insider nodes.

It's worth noting that, the final format of the global trust value $T_m(i)$ where $i \in \{Packet\_Tamper, Packet\_Drop\}$, is a pair of real numbers locating in the interval $[0, 1]$, they can also be considered as probabilities. The global trust value thus can be indicated by the accumulative packet drop ratio and packet tamper ratio of the insider node m. The significance of calculating the global trust comparing to the local trust is that: in the global trust, the sample space which covers all the routes that utilized the insider node m, is much richer than the sample space for single route's local trust evaluation. According to the *Law* *of Large Numbers*[36], the average of the results obtained from a large number of trials should be close to the expected value, and will tend to become closer as more trials are performed. Therefore, the integrated global trust is more close to the real probability that each insider node drops (tampers) data packets.

4 Game-Based Analysis for Trust Policies

In this section, the proposed trust management mechanism is analyzed by game theory. The trust policy is made to distinguish the malicious, suspicious, and legitimate insider nodes based on the game equilibrium. The reason for utilizing game theory for the trust decision making is owing to the tradeoff existing in the communication phase. For instance, by dropping or tampering packets, the attacker may receive illegal utility, but may also take risk of being punished. For the cluster head, it can severely punish an insider node for its losing a little packet, but the usability of the network will decrease. Therefore, the interaction between the cluster head and the insider node is a multi-dimensional decision making problem which is often modeled and analyzed as a game[35].

4.1 Trust Game Model

In clustered WSNs, the game is between any one of the insider attackers who takes attack strategies, and 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[34]. The first step of game theory based analysis is to identify the players and their available actions (or strategy). The insider node is perfectly informed of the historical strategies of the cluster head, for the reason that the strategy of the cluster head, which is the global trust value, has been broadcasted to all the members in the network including the insider attacker. On the contrary, the insider's past strategies are not perfectly observed by the cluster head, because the observation mechanism is not perfectly accurate. Moreover, because the cluster head takes its strategy after the insider, we construct the game in an extensive form.

Fig.1 portrayed 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 defence 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

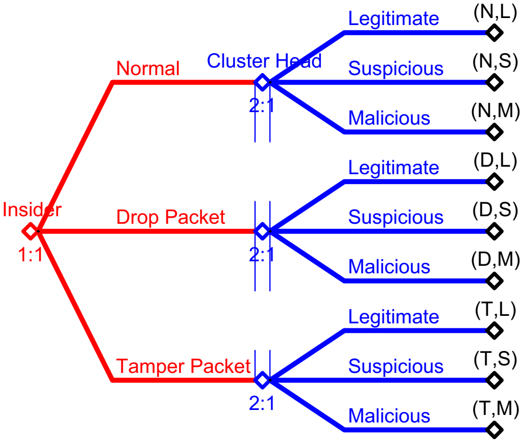

Fig. 1. Extensive Form of Trust Game

completely distrust the insider, classify it as *Malicious*(M). Since there is no observation mechanism with 100% detection rate[21], the cluster head is not totally certain that the insider chooses one of the strategies from its strategy space. Therefore, the cluster head's 3 sub-trees belong to the same information set, which is illustrated by a dash line linking the 3 blue nodes. After both the attacker and the cluster head choose their own strategies to fight against each other, the interaction between these two players will come to an outcome, which are denoted by different leave nodes in the end of the game tree. We can see that there are totally 9 leaf nodes at the end of the extensive game tree which identify all the possible outcomes (3×3) of the one-shot trust game. The following items describe the meanings of all the possible outcomes of this trust game.

- (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 above outcomes is denoted as $U_m(u, v)$, where $u \in \{Normal(N), Drop(D), Tamper(T)\}$ is the strategy from insider, and $v \in \{Legitimate(L), Suspicious(S), Malicious(M)\}$ is the strategy of the cluster head. Since in the clustered wireless sensor network, the attacker's gain is the same as 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[35]. We illustrate the utilities for the cluster head (the network) at different outcomes as the matrix in the following table, in which the $U_n(u, v)$ may vary in different application scenarios[20]. For example, the damage from a tampered data packet in the battle field sensor network will be much more severe than the damage in the civilian applications.

Table 1. Different Payoffs for Network at Different Outcomes

Strategy	*Trust(Legitimate)*	*Semi-Trust(Suspicious)*	*Distrust(Malicious)*
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	$U_n(T, L)$	$U_n(T, S)$	$U_n(T, M)$

In Table 1, the first elements in each utility function are actions of the insiders, while the second elements are the actions of the cluster head. For example, $U_n(T, M)$ is the utility for the cluster head under the situation that the insider node tampers a packet, and the cluster head classify it as malicious and distrust it. It is worth noting that, $U_n(u, v)$ is the utility under *pure strategy.* In game theory, the notion of pure strategy means the players choose the strategies deterministically. That is to say, the players choose each strategy with probability 0 or 1. However, in the real case, the rational attacker will change its strategy over time, and sometimes just pretends to be legitimate and takes the malicious strategy with certain probability. This kind of rational attacker will choose each possible strategy with a certain probability. Thus, the trust game is a mixed-strategy game, in which the player's strategy is probability distribution over the action set.

Table 2 illustrates the mixed strategy for both the attacker and the cluster head. In this mixed strategy game, the attacker's strategy is a probability distribution $\{p, q, 1 - p - 1\}$ over all its possible action set $\{N, D, T\}$. Variables p, q, $1 - p - q$ are the probabilities for the attacker to adopt each of the actions *Behave Normally*$(u = N)$, *Drop Packet*$(u = D)$, and *Tamper Packet*$(u = T)$, respectively. On the contrary, for the cluster head, its strategy is a probability distribution $\{x, y, 1 - x - y\}$, over the cluster head action set $\{L, S, M\}$. Here x,

Table 2. Joint Distribution for Attacker and Cluster Head's Mixed Strategy

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

y, $1-x-y$ are the probabilities for the cluster head to classify the insider node as *Legitimate*$(v = L)$, *Suspicious*$(v = S)$ and *Malicious*$(v = M)$, respectively. The mixed strategy of the insider attacker is denoted as $s_m(p, q)$ which is a probability distribution over action set $\{Normal, Drop, Tamper\}$, while m denotes this potential attacker. And the mixed strategy for the cluster head is $s_n(x, y)$ which is a probability distribution over $\{Legitimate, Suspicious, Malicious\}$, while n indicates the cluster head. The combination in each grid in the Table.2 is the joint probability for both the attacker and the defender to choose certain actions. For example, the grid for $(1 - p - q)(1 - x - y)$ means the joint probability that the attacker tamper the packet while the cluster head classify it as malicious at the same time. The matrix in Table.2 is thus the joint probability distribution for each possible outcome.

4.2 Trust Game Equilibrium

In the last subsection, we have construct the trust game model based on the *Attack-Defence* interaction between the insider node and the cluster head. To find the optimal defense strategy for the cluster head, we need to analyze this trust game. The key point in the game analysis is to find the Nash equilibrium[31]. For this trust game, the Nash equilibrium points indicates the outcome in which neither the insider nor the cluster head wants to unilaterally change its strategy. Otherwise, the unilateral change of the strategy will only lead to its own utility degradation[34, 35]. 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[6, 35]. This min-max decision rule, in zero-sum game theory, is well known as the necessary and sufficient condition for the Nash equilibrium[34].

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:

$$\begin{cases} s^*_m(p,q) = \arg \min\limits_{s_m(p,q)} \max\limits_{s_n(x,y)} \mathbb{E}_m\left(s_n(x,y), s_m(p,q)\right); \\ s^*_n(x,y) = \arg \max\limits_{s_n(x,y)} \min\limits_{s_m(p,q)} \mathbb{E}_m\left(s_n(x,y), s_m(p,q)\right). \end{cases} \tag{7}$$

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 dominant mixed strategy of the attacker. $\mathbb{E}_m\left(s_n(x,y), s_m(p,q)\right)$ 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 [34], 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.

4.3 Trust Game Evolution

In last section, we analyzed the trust game within single time window $TW(t)$. 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)[33] 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:

$$P_i^k = \frac{\exp(\lambda \times EU_i^k(P_{-i}))}{\sum_m \exp(\lambda \times EU_i^m(P_{-i}))} \tag{8}$$

where P_i^k is the probability for player choosing strategy k, which is the same as the p, q and $1-p-q$ (or x, y and $1-x-y$) in the one-shot trust game. $EU_i^k(P_{-i})$ 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. Table 3 in Appendix shows the relationship between the strategies and the value of λ.

We consider the trust mechanism confronting 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 methord[37], 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 attacker will attach more importance on bring 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[37], the example utilities $U_n(i, j)$ are defined. Then by using the tool GameBit[38], the QRE of the repeated trust game is derived.

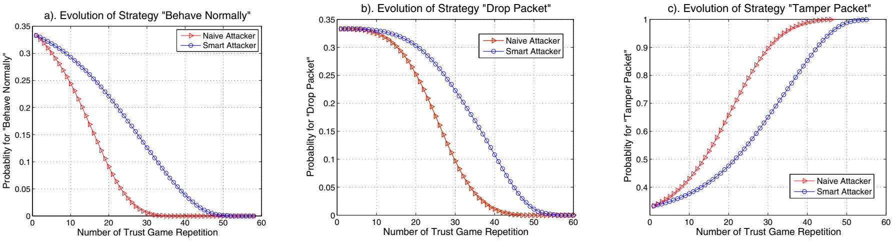

Fig. 2. Comparison of Strategy Evolution of the Smart and Naive Attackers

Fig.2 illustrates the strategies' evolution of the smart and naive attackers. 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 number of time window $TW(t)$ increases, the trust game 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. Based on this analysis, 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.

Fig.3 illustrates the co-evolution of the strategies of smart attacker and cluster head while they play the trust game. From Fig.3(a) we can see: with the game repeats, the attacker prefers more to tamper packet, but gradually decreases the probability for dropping packets. This is because while time goes on, the risk of being detected also increases. Therefore the attacker does not want to take the risk of being considered as malicious for dropping packets. In Fig.3(b) we can see that, more repetitions of the trust game will give the cluster head more information to increase the detection accuracy. Therefore, the probability for wrongly classify the attacker as legitimate (green line) consecutively decreases. Noting that the blue line first increases to a peak value, but then decreases, finally even reaches to value 0. This interesting phenomena indicates significantly that: during the first period (before step 15), due to lack of observation, the cluster head can not make decision that the insider node is a smart attacker.

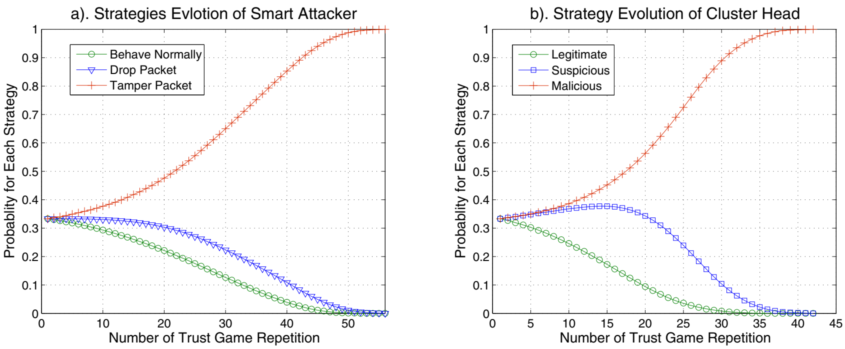

Fig. 3. Attacker and Cluster Head's Strategy Evolution

However, it becomes more suspicious of this insider attacker. With the trust game repeats, it obtains more and more information of the smart attacker's misbehavior. Therefore, it decidedly decreases the probability for the strategy for classifying the insider node as *Suspicious* and *Legitimate*, but increases the probability to identify it as a malicious attacker. More data about the trust game's co-evolution is illustrated in Table 3 in the appendix.

5 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 malicious and suspicious insider attacker to minimum. The future work is to implement this trust management mechanism, design an effective intrusion detection system for WSNs by taking into consideration of false positive rate and false negative rate.

Acknowledgements. This work is partly supported by Grants-in-Aid for Scientific Research (B) (23300027), Japan Society for the Promotion of Science (JSPS). The first author Dong HAO is supported by the governmental scholarship from the China Scholarship Council (CSC). The second author Dr. Avishek

Adhikari's visit to Kyushu University is sponsored by the Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields Supported by Japan Science and Technology Agency and Department of Science and Technology of the Government of India.

References

1. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Computer Networks 52(12), 2292–2330 (2008)
2. Perrig, A., Stankovich, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM 47(6), 53–57 (2004)
3. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized Trust Management. In: Proceedings of the 17th IEEE Symp. on Security and Privacy, pp. 164–173. IEEE Computer Society (1996)
4. Josang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst., 618–644 (March 2005)
5. Josang, A., Hayward, R., Pope, S.: Trust network analysis with subjective logic. In: Proceedings of the 29th Australasian Computer Science Conference (ACSC 2006), Darlinghurst, Australia, vol. 48, pp. 85–94 (2006)
6. Gollmann, D.: From Access Control to Trust Management, and Back – A Petition. In: Wakeman, I., Gudes, E., Jensen, C.D., Crampton, J. (eds.) IFIPTM 2011. IFIP AICT, vol. 358, pp. 1–8. Springer, Heidelberg (2011)
7. Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: Proceedings of ACM Security for Ad-hoc and Sensor Networks, SASN (2004)
8. Shaikh, R.A., Jameel, H., Brian, J., Lee, H., Lee, S., Song, Y.J.: Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 1698–1712 (November 2009)
9. Momani, M., Challa, S., Alhmouz, R.: Can we trust trusted nodes in wireless sensor networks? In: International Conference on Computer and Communication Engineering (ICCCE 2008) (May 2008)
10. Lin, C., Vijay, V.: A Hybrid Trust Model for Enhancing Security in Distributed Systems. In: The Second International Conference on Availability, Reliability and Security, pp. 35–42 (2007)
11. Aivaloglou, E., Gritzalis, S.: Hybrid trust and reputation management for sensor networks. Wirel. Netw. 16(5) (July 2010)
12. Spyropoulos, T., Psounis, K., Raghavendra, C.S.: Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case. IEEE/ACM Transactions on Networking 16(1), 63–76 (2008)
13. Gómez, F., Girao, J., Pérez, G.M.: TRIMS, a privacy-aware trust and reputation model for identity management systems. Comput. Netw. 54(16) (November 2010)
14. Shila, D.M., Cheng, Y.: Mitigating selective forwarding attacks with a Channel Aware Approach in WMNs. IEEE Transaction on Wireless Communications (May 2010)
15. Ellison, C.M., Franz, B., Rivest, R., Thomas, B.M., Ylonen, T.: Simple public key infrastructure certificate theory. IETF RFC 2693 (1999)
16. Freudenthal, E., Pesin, T., Port, L., Keenan, E., Karamcheti, V.: dRBAC: Distributed role-based access control for dynamic coalition environments. Technical Report, TR 2001-819, New York University (2001)

17. Velloso, B., Laufer, P., Duarte, O., Pujolle, G.: A Trust Model Robust to Slander Attacks in Ad Hoc Networks. In: Proceedings of 17th International Conference on Computer Communications and Networks (ICCCN 2008), pp. 1–6 (2008)
18. Lynch, D.M.: Securing against insider attacks. Information Security Systems 15(5), 39–47 (2006)
19. Kantzavelou, I., Katsikas, S.: A game-based intrusion detection mechanism to confront internal attackers. Computers Security 29(8), 859–874 (2010)
20. Anjum, F., Mouchtaris, P.: Security for Wireless Ad Hoc Networks. Wiley-Interscience (2007) ISBN:0471756881
21. Bace, R.G.: Intrusion detection. Macmillan Publishing Co., Inc., Indianapolis (2001)
22. Xue, X.Y., Leneutre, J., BenOthman, J.: A Trust-based Routing Prtocol for Ad Hoc Networks. In: Proceeding of Mobile and Wireless Communications Networks, pp. 251–262 (October 2004)
23. Royer, E.M., Toh, C.K.: A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications, 46–55 (April 1999)
24. Bao, F., Chen, I.-R., Chang, M., Cho, J.: Hierarchical trust management for wireless sensor networks and its application to trust-based routing. In: Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1732–1738. New York (2011)
25. Scott, K., Bambos, N.: Routing and channel assignment for low power transmission in PCS. In: Proc. IEEE ICUPC 1996, vol. 2, pp. 498–502 (1996)
26. Singh, S., Woo, M., Raghavendra, C.S.: Power-aware routing in mobile ad hoc networks. In: Proc. ACM MobiCom 1998, pp. 181–190 (1998)
27. Toh, C.-K.: Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks. IEEE Communications Magazine, 138–147 (June 2001)
28. Li, H., Singhal, M.: Trust Management in Distributed Systems. Computer, 45–53 (February 2007)
29. Xiong, L., Liu, L.: Building Trust in Decentralized Peerto- Peer Electronic Communities. In: Proc. 5th Intl. Conf. Electronic Commerce Research (ICECR-5) (2002)
30. Hao, D., Ren, Y., Sakurai, K.: A Game Theory-Based Surveillance Mechanism against Suspicious Insiders in MANETs. In: Chen, L., Yung, M. (eds.) INTRUST 2010. LNCS, vol. 6802, pp. 237–252. Springer, Heidelberg (2011)
31. Liu, D., Wang, X.F., Camp, J.L.: 'Game Theoretic Modeling and Analysis of Insider Threats. International Journal of Critical Infrastructure Protection, 75–80 (2008)
32. Pirzada, A.A., Mcdonald, C., Datta, A.: Performance comparison of trust-based reactive routing protocols. IEEE Transactions on Mobile Computing 5(6), 695–710 (2006)
33. Richard, M.K., Thomas, P.: Quantal Response Equilibria for Extensive Form Games. Experimental Economics 1, 9–41 (1998)
34. Gibbons, R.: Game Theory for Applied Economics. Princeton University Press, Princeton (1992)
35. Alpcan, T., Basar, T.: Network Security: A Decision and Game Theoretic Approach, November 30. Cambridge University Press (2010)
36. Mitzenmacher, M., Upfal, E.: Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press, New York (2005)
37. Binmore, K.G.: Playing for real: a text on game theory. Oxford University Press (2007) ISBN 0195300572, 9780195300574
38. McKelvey, R.D., McLennan, A.M., Turocy, T.L.: Gambit: Software Tools for Game Theory, Version 0, September 01 (2010), http://www.gambit-project.org

Appendix: Quantal Response Equilibria of Trust Game

Table 3. Quantal Response Equilibria (QRE) Calculations

		Insider Attacker			Cluster Head		
Step	λ	Normal	Drop	Tamper	Legitimate	Suspicious	Malicious
1	0.000	0.333	0.333	0.333	0.333	0.333	0.333
2	0.008	0.330	0.333	0.337	0.327	0.337	0.337
3	0.016	0.326	0.333	0.340	0.319	0.340	0.341
4	0.025	0.322	0.333	0.344	0.311	0.344	0.345
5	0.035	0.318	0.333	0.349	0.302	0.348	0.350
...	...	...	...	...	...	...	...
12	0.126	0.281	0.328	0.391	0.218	0.374	0.408
13	0.143	0.274	0.326	0.399	0.203	0.376	0.421
14	0.161	0.268	0.324	0.408	0.188	0.377	0.436
15	0.180	0.261	0.322	0.418	0.172	0.377	0.452
16	0.200	0.253	0.319	0.428	0.156	0.375	0.470
17	0.221	0.246	0.316	0.439	0.140	0.371	0.490
18	0.242	0.238	0.312	0.450	0.124	0.364	0.512
19	0.265	0.229	0.308	0.463	0.109	0.355	0.536
20	0.289	0.221	0.303	0.476	0.094	0.343	0.563
...	...	...	...	...	...	...	...
36	0.802	0.070	0.157	0.772	0.000	0.014	0.985
37	0.852	0.062	0.145	0.793	0.000	0.009	0.991
38	0.907	0.054	0.133	0.813	0.000	0.005	0.995
39	0.967	0.046	0.121	0.833	0.000	0.003	0.997
40	1.033	0.039	0.108	0.853	0.000	0.002	0.998
41	1.105	0.032	0.096	0.872	0.000	0.001	0.999
42	1.184	0.026	0.083	0.891	0.000	0.000	1.000
...	...	...	...	...	...	...	...
47	1.732	0.005	0.030	0.964	0.000	0.000	1.000
...	...	...	...	...	...	...	...
54	3.216	0.000	0.002	0.998	0.000	0.000	1.000
55	3.529	0.000	0.001	0.999	0.000	0.000	1.000
56	3.874	0.000	0.000	1.000	0.000	0.000	1.000