2008 International Symposium on Computer Science and Computational Technology

A New Security Mechanism Based on SIP in Wireless LAN-3G Integration

Hui Lin
Key Laboratory of Network Security and Cryptology
Fujian Normal University
Fuzhou, China
Hawkhui95@gmail.com

Li Xu, XiaoDing Wang
Key Laboratory of Network Security and Cryptology
Fujian Normal University
Fuzhou, China
xuli@fjnu.edu.cn

***Abstract*—The traditional security enforcement approach of network is employing cryptography and authentication scheme. However, we consider that the conventional view of security based on cryptography alone is not sufficient for the wireless LAN and Third-generation (3G) integration networks against malicious or non-malicious insertion of data from internal adversaries or faulty nodes. In this paper, we propose a trust degree-based dynamic model for wireless LAN and 3G integration networks where nodes maintain trust degree for other nodes meanwhile the trust degree is applied to evaluate their trustworthiness. Finally the conclusion is made by verifying the performance of this model through some preliminary simulation results.**

Keywords-Wireless LAN; 3G; Security; Trust Degree; Session Initial Protocol

I. INTRODUCTION

Third-generation (3G) cellular systems will provide global coverage and nearly universal roaming, offering data rates up to 2 Mb/s. However the grawback is obvious, deployment and management cost a lot. On the other hand, wireless LAN (WLAN) systems are more suitable for hotspot coverage and offer data rates that easily exceed 3G data rates with low investment cost. Hence, integrating the two systems would allow operators to take advantage of their best features.

A typical way to consider the integration of 3G with WLAN is to give access to resources and services offered by a 3G system using a terminal with a WLAN interface [1]. However, security problems also arise. WLAN and 3G are usually very accessible within the physical world, and the capability of a WLAN-3G network performing its task depends not only on its ability to communicate among the nodes, but also on its ability to collectively processing information. This decentralized in-network decision-making, which relies on the inherent trust among the nodes, can be abused by adversaries to carry out security breaches through compromised nodes and makes them very vulnerable.

Now, there have been several proposals, all of which based on cryptography, to ensure secure communication on these resource constrained nodes such as INSENS, SERP, SEF etc. The establishment and management of cryptographic keys [2] form the backbone of these schemes. But either of cryptographic and authentication mechanisms alone cannot be used to solve the problem about trust as internal adversarial nodes have accessed to valid cryptographic keys. Thus, providing secure WLAN-3G based on trust becomes very important.

Trust-management approach for distributed systems security [3] was first introduced with the context of Internet as an answer to the inadequacy of traditional cryptographic mechanisms. Some of the notable earlier works in this domain had been done about trust-management engines such as KeyNote [4] and RT framework [5]. Since then, trust degree-based frameworks based on the approach of trust management are extensively studied in many contexts and equally diverse domains such as human social networks, ecommerce, 802.11 networks, peer-to-peer networks etc.

In this paper, we propose a dynamic trust model for WLAN-3G by employing Bayesian network combined with beta trust degree and extend the session initial protocol (SIP) to implement and validate the proposed model.

The paper is organized as follows. Section II discusses the register process in WLAN-3G. Section Ⅲ the proposed dynamic trust security model in WLAN-3G is presented. Section IV describes the simulation and performance analysis. Finally conclusions are drawn in Section V.

II. REGISTER PROCESS IN WLAN-3G

The dynamic trust model based WLAN-3G integration architecture is shown in Figure 1[6][7]. In this architecture, the user could have his/her 3G user agents(UA) switched on and registered to the CS/PS/IMS 3G domains, and in parallel have his/her mobile terminal (MT) accessed to a WLAN hotspot and then registered to the 3G domains. In this paper we only consider the process of WLAN MT registering to the WLAN-3G.

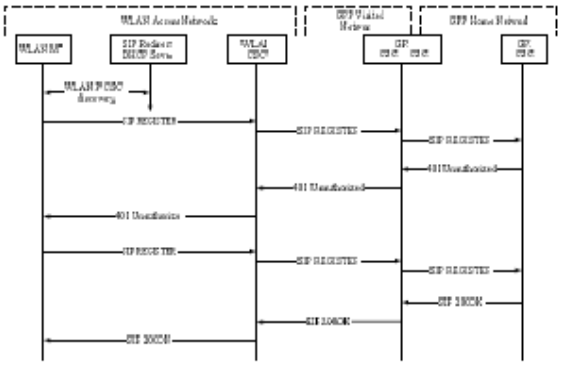


Figure 1. WLAN-3G Integration Architecture

978-0-7695-3498-5/08 $25.00 © 2008 IEEE
DOI 10.1109/ISCSCT.2008.23

The register process of WLAN MT in this architecture is based on SIP as shown in Figure 2.

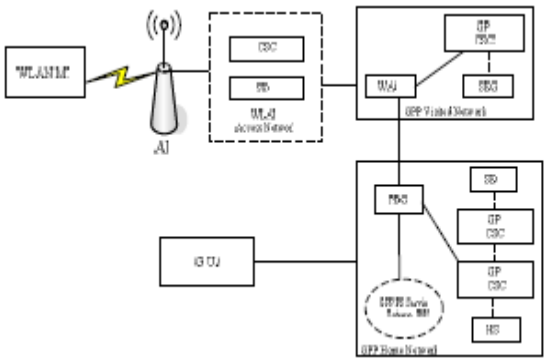


Figure 2. WLAN MT Register Process in WLAN-3G

In this process, when a MT roams onto a new network, first it tries to associate with a wireless Access Point (AP). After the association with the AP the MT dynamically configures its IP layer by means of DHCP function implemented in the WLAN access network. The DHCP server will provide the MT together with basic IP configurations under service related to configuration --the default outbound proxy P-CSCF.

Since in this initial phase the MT is still filtered by the WLAN access router/SEG, the SIP REGISTER request is sent through the WLAN access network P-CSCF.

Upon receiving the new SIP REGISTER request, the WLAN P-CSCF indicates in the SIP authorization header that the request was received through a protected connection. Then the WLAN P-CSCF determines the next hop and forwards the request. If the wireless access network is federated or belongs to a foreign 3G network the next hop will be a 3GPP visited network P-CSCF while if the wireless access network belongs to or is federated to the user's home 3G network, the next hop will be a 3GPP home network I-CSCF or directly the 3GPP home network S-CSCF. The request is then routed via 3GPP P-CSCF/I-CSCF to the 3GPP S-CSCF as defined for IP Multimedia Subsystems (IMS).

Upon receiving the SIP REGISTER the 3GPP S-CSCF identifies the user. If the check is successful then the user has been authenticated. The S-CSCF then sends back a 200 "OK" SIP response to the MT. When the WLAN P-CSCF receives the 200 "OK", it instructs the access router/SEG to modify its firewall rules in order to enable network connectivity to the authenticated MT, and forwards the response to the MT. On receiving the "200 OK" response, the MT use the newly established set for exchanging messages with the SEG/WLAN P-CSCF and then the process of MT registering to the 3G domain based on SIP is complete.

III. DYNAMIC TRUST SECURITY MODEL IN WLAN-3G

According to the architecture and register process mentioned in section Ⅱ, we set up a trust model between a truster and a trustee by employing a Bayesian formulation with beta distribution according to the Saurabh Ganeriwal and Laura K 's approach [8]. The proposed trust model takes into account both direct and indirect trust between nodes.

In the proposed trust model, we first define a data structure containing the form (α_j, β_j) in node i, termed as the trust degree table, TDT_i, that stores the trust degrees corresponding to every node j maintained by node i.

$$TDT_i = \{TD_{ij}\} \tag{1}$$

Then we define a parameter TD_{ij} to represent the trust degree of node j maintained by node i. Trust degree is maintained as a probabilistic distribution, enabling the node to have full freedom and not get constrained by some discrete levels of trust degree [9]. A node builds each entry in the trust degree table over time through the SIP REGISTER message. The interaction between the two blocks is given by equation (2); the information carried by the SIP REGISTER message, SR_{ij} mapped to a pair of (r,s), is used to recursively update the trust degree of node j at node i, TD_{ij}.

$$TD_{ij} = F(SR_{ij}, TD_{ij}) \tag{2}$$

Qualitatively, SR_{ij} represents the rating that is allocated to the latest action of node j by node i and F(.) is responsible for updating the trust degree of node j in light of the new observation.

In the proposed model, we consider both direct and indirect trust between nodes as follows:

$$(TD_{ij})_D = F\lfloor SR_{ij}, (TD_{ij})_D \rfloor \tag{3}$$

$$(TD_{ij})_{ID} = (TD_{ij})_{ID} + (TD_{kj})\forall k \in N_i \tag{4}$$

Direct trust degree, $(TD_{ij})_D$, is build up using direct observations through the SIP REGISTER message and indirect trust degree, $(TD_{ij})_{ID}$, is build up using indirect observation respectively.We will quantitatively define the trust degree and trust in following contents.

A. Modeling Trust degree & Trust

Define 1: The trust degree of a node in the proposed trust model can be represented by beta distribution.

Proof: The beta distribution is indexed by two parameters (α, β). It can be expressed using the gamma function as:

$$P(x) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{(\alpha-1)}(1-x)^{(\beta-1)}$$
$$\forall 0 \le x \le 1, \alpha \ge 0, \beta \ge 0 \tag{5}$$

Assume: (1) a node rates the behavior of another node during every transaction on a binary scale (cooperative

(1), noncooperative(0));(2) node i had interacted with node j in m+n events; out of which it characterizes m and n interactions to be cooperative and non-cooperative respectively.

Given these information, node i want to predict the behavior of node j (cooperative/non-cooperative), θ, for the next event. Clearly, without any prior information, θ is uniformly distributed over the measurement space, (0,1). Thus, P(θ)=uni(0,1)=Beta(1,1). Using the binary rating model, we can model the prior interactions using a binomial distribution and then the posterior distribution of θ can be calculated as the method in [10][11]:

$$P(\theta) = \frac{Bin(m+n,m) * Beta(1,1)}{normalization} = Beta(m+1,n+1) \quad (6)$$

Equation (6) shows that the posterior distribution of θ is a beta distribution which justifies the define 1.

According to the define 1, the trust degree of node j maintained at node i without getting any information from the SIP REGISTER is given as equation (7):

$$TD_{ij} = Beta(\alpha_j + 1, \beta_j + 1) \quad (7)$$

Here α_j and β_j represents the cooperative and non-cooperative interactions between node i and j respectively (from the perspective of node i). Without any prior observations, $\alpha_j = \beta_j = 0$ and hence, TD_{ij} = Beta(1,1) = uni(0,1).

Then the trust of a node is the statistical expectation of the trust degree function and is given by:

$$T_{ij} = E(TD_{ij}) \quad (8)$$

B. Updating Trust degree for Direct Trust

In equation (7) we quantify the trust degree at node i statically without considering the information carried by SIP REGISTER message. In order to make our trust model dynamic, we propose a method for trust degree update when a node makes some direct observations from the SIP REGISTER message.

We assume that: (1) node i has build up some trust degree metric, TD_{ij}, for node j. (2) Node i again interacts with node j for r+s more events, r cooperative and s non-cooperative; (3) r and s to be integers. The trust degree can be updated as:

$$TD_{ij} = Beta(\alpha_j + r + 1, \beta_j + s + 1) \quad (9)$$

From the equation (9), we can find that the trust degree update is equivalent to just updating the value of the two parameters α_j and β_j as follows:

$$\alpha_j^{new} = (\omega * \alpha_j) + r; \beta_j^{new} = (\omega * \beta_j) + s \quad (10)$$

Here, ω, termed as aging weight, can take values in the range (0, 1). It is responsible for making sure that all the nodes cooperate at all the time. A malicious node can very well choose a strategy of cooperating at the start and then abusing the system thereafter using the trust degree that it has acquired initially. An appropriate choice of the aging weight will make sure that trust degree information become stale and make a node to maintain a good trust degree continuously.

C. Updating Trust degree for Indirect Trust

If node i receives trust degree information about node j through node k, then let us represent these indirect observations by (α_j^k , β_j^k). Node i already have prior trust degree information about j and k, represented by (α_j, β_j) and (α_k, β_k) respectively. We need to combine these pieces of information to obtain new trust degree information of j, (α_j^{new} , β_j^{new}). With the Dempster-Shafer belief theory [12] and the concept of belief discounting [13], The trust degree update for indirect trust, as derived in [10], are given by the following equations:

$$\alpha_j^{new} = \alpha_j + \frac{\{2 * \alpha_k * \alpha_j^k\}}{\{(\beta_k + 2) * (\alpha_j^k + \beta_j^k + 2)\} + \{2 * \alpha_k\}}$$
$$\beta_j^{new} = \beta_j + \frac{\{2 * \alpha_k * \beta_j^k\}}{\{(\beta_k + 2) * (\alpha_j^k + \beta_j^k + 2)\} + \{2 * \alpha_k\}} \quad (11)$$

D. Identification and Isolation of Malicious Nodes

When facing with the question of identifying and isolating a malicious node i, the decision of node i, (D_{ij}), is derived from the trust between the two nodes. We use a simple threshold based policy to decide the value of D_{ij} as equation (12):

$$D_{ij} = \begin{cases} Trustworthy \forall T_{ij} \geq TH \\ Distrustworthy \forall T_{ij} < TH \end{cases} \quad (12)$$

The actual decision of node i will depend on D_{ij}. If the D_{ij} less than the TH, the node i can identify that the node j is a malicious node and rejects the register request from node j. At the same time, node i will exchange the trust degree information with other nodes in the networks.

IV. Performance Analysis

A. SIP extension for Dynamic Trust Security Mechanism

As mentioned in section Ⅲ, the SIP Registration procedure has been used as generic register method for a MT to connect to the 3G domain via WLAN, 3GPP visited / home networks in the proposed dynamic trust model. In

order to simplify the proper access networks class selection (3GPP home, visited, none, etc.), a common solution should be used. In this section a simple mechanism is proposed for the MT to indicate which access networks it is willing to access. The mechanism makes use of the SIP extension defined within the IETF, which allow a user agent to convey its capabilities and characteristics to other user agents and servers[14][15].

We extends SIP by defining two new parameters (integer numbers) "ci" and "nci" indicating "cooperative interaction" and "non cooperative interaction" in contact header filed of the REGISTER message[16]. The two values of the parameters are completely implementational dependent and are taken in integer.

For example, an MT fills the following Contact header within the REGISTER message as:

Contact:<sip:hawk@192.168.1.2>;mobility="mobile";ci =0";nci="0"

With the parameters "from", "to", "contact ci nci" we can judge the information carried by this REGISTER message is direct or indirect, also we can use the values of these parameters to judge weather it is trustworthy or not.

B. Simulation and Performance Analysis

For trust degree based networks such as WLAN-3G, ad-hoc networks or mesh are highly susceptible to identity attacks such as denial of service attack. So in this section, we will compare the performance of identity attacks and defense between traditional authentication mechanisms and our dynamic trust mechanism.

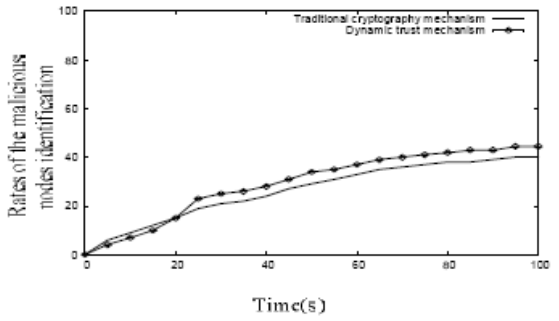
We implement our design in two scenarios by NS2. The simulation environment setting is shown in table1. In scenario (a), 30% of nodes in the network are malicious, only around 70% of attempts to build a sufficient trust relationship are successful which is as same as the percentage of honest nodes in the network. In scenario (b), we simulate a network with 70% of the nodes malicious that represents a hostile network condition in (b). In addition, nodes in the network do not know each other at the beginning and no packet is dropped due to network ambiguities.

TABLE I. SIMULATION ENVIRONMENT SETTING

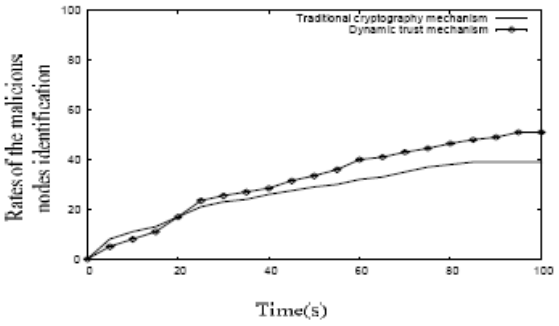
Simulation parameter	Parameter value
Node Number	50
Area	1000m*1000m
Time	100s
Channel capcity	2Mbits
Mac protocol	IEEE 802.11
Initial α_j, β_j	0
Initial ci, nci	1,0
ω	0.98
TH	0.9

The two simulation results show in Figure 3 (a) and (b). It can be found that nodes take some time to build up the trust relationships among them at the beginning. So in the first 20 seconds, the malicious nodes identification rate of traditional mechanism is better than the dynamic trust model. However, in the spare time, weather in a commonly network or in a hostile network, the proposed dynamic trust model both does better than traditional cryptography and authentication mechanism in identifying the malicious nodes, especially in the hostile network.

The results of the two experiments show that the proposed dynamic trust model can improve the security of the WLAN-3G integration network efficiently.



(a)



(b)

Figure 3. Rates of the malicious nodes identification

V. CONCLUSION

Cryptography presents an efficient mechanism for node authentication and maintaining data confidentiality and integrity. We highlight some novel characteristics of WLAN-3G integration networks leading to unconventional attacks and system failures where cryptographic solutions are not sufficient. On the basis of these observations, we propose a dynamic trust model based on Bayesian formulation and beta distribution for developing a community of trustworthy nodes at runtime. The performance of the proposed model is verified through the simulation, by which we claim that the proposed dynamic trust model provides a practical solution for developing WLAN-3G integration networks.

ACKNOWLEDGMENT

This work is supported Partially by Natural Science Foundation of China (NO.60502047), key Science Foundation of Fujian High University in China (NO.JA07030) and Natural Science Foundation of Fujian Province (NO.2008J0014)

REFERENCES

[1] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[2] L. Veltri , S. Salsano , G. Martiniello. Wireless LAN-3G Integration: Unified Mechanisms for Secure Authentication based on SIP. IEEE ICC 2006,p2219-2224

[3] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In Proceedings of IEEE Conf. Security and Privacy, 1996, Oakland, California, USA. p234 - 245.

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

[5] N. Li, J. Mitchell, and W. Winsborough. Design of a rolebased trust management framework. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland.p145-152

[6] K. Ahmavaara, H. Haverinen, R. Pichna, "Interworking Architecture between 3GPP and WLAN Systems", IEEE Communications Magazine, November 2003.p120-127

[7] G. M. Køien and T. Haslestad. "Security Aspects of 3G-WLAN Interworking". IEEE Communications Magazine, November 2003.p134-145

[8] Saurabh Ganeriwal, Laura K. Balzano, Mani B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks", ACM Transactions on Sensor Networks, Vol. V, No. N, March 2007, Pages 1-37.

[9] K. Krukow and A. Twigg, "Distributed Approximation of Fixed-Points in Trust Structures," Proc. of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), June 2005.p805 - 814.

[10] A. Jsang and R. Ismail. The Beta Reputation System. In Proceedings of the 15th Bled Electronic Commerce Conference, June 2002. p213-219

[11] Beta distribution from Mathword. http://mathworld.wolfram.com/BetaDistribution.html

[12] G. Shafer. A mathematical theory of evidence. Princeton University, 1976.

[13] A. Jøsang. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, June 2001 9(3).p279–311.

[14] J. Rosenberg et al., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[15] J. Rosenberg, C. Jennings, "The Session Initiation Protocol (SIP) and Spam", draft-ietf-sipping-spam-03, internet draft (work in progress), October 2006

[16] J. Peterson, C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-06 (work in progress), October 2005.