Scientific Research and Essays Vol. 6(18), pp. 3873-3884, 1 September, 2011
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE11.440
ISSN 1992-2248 ©2011 Academic Journals

Full Length Research Paper

A subjective logic based dynamic trust mechanism for voice over internet protocol (VOIP) over wireless mesh networks (WMNs)

Hui Lin[1], Li Xu[1*], Jianliang Gao[2] and Kai Yang[3]

[1]Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China.
[2]School of Computing and Mathematics, University of Ulster, Jordanstown, Co. Antrim BT37 0QB, UK.
[3]School of Computer Science, Xidian University, Xian, 710071, China.

Accepted 27 June, 2011

Voice over internet protocol (VoIP) service has been a very popular and important application over the internet. Wireless VoIP also becomes more and more popular due to its features of low cost and convenience. Wireless mesh networks (WMNs) have emerged as a key technology for the next-generation wireless networks and have been considered as a good solution for VoIP services due to deployment and wide coverage. However, there have been raised relevant security concerns referred to integrating IP Telephony into existing applications and system infrastructure. One of the critical concerns is how to enhance the security of session initiation protocol (SIP) and security among the nodes by blocking identity spoofing and preventing various attacks in the convergent communication systems in WMNs, which are usually deployed under the assumption that participating nodes cooperate with each other. In this paper, we propose a subjective logic based dynamic trust mechanism for securing the SIP-based VoIP over WMNs. The dynamic trust mechanism incorporates uncertainty in association with subjective logic into the reputation computation to detect and isolate the existing malicious nodes. Also, it considers the quality of wireless links which can differentiate intentional packet drop from packet drop due to poor link quality and give accurate detection even in presence of poor wireless links. We demonstrate the performance of the dynamic trust mechanism through network simulator (NS) 2 simulations.

Key words: WMN, subjective logic, security, SIP, VoIP, dynamic trust.

INTRODUCTION

For the sake of cost saving and convenience, voice over internet protocol (VoIP) services have recently been more and more common in commercial and civil communications. Recent years have witnessed the phenomenal growth of VoIP (Ruishan et al., 2010; Perez, 2009a). During the last few years, there has been a steady market shift from the circuit switched plain old telephone system (POTS) to the VoIP telephony (Perez, 2009b; Enterprise VoIP Adoption, 2009; Higdon, 2009). International data corporation (IDC) reported that the number of United States residential VoIP subscribers has grown from 10.3 million in 2006 to 44 million in 2010. Status quo shows that VoIP will gradually replace the public switched telephony network (PSTN) and govern the future telecommunication market (Barnard, 2009a). Application binary interface (ABI) (Barnard, 2009b) predicted that the number of worldwide residential VoIP subscribers will exceed 267 million by 2012. On the other hand, wireless networks have the advantages of low cost and mobility. Deploying VoIP over wireless networks has the significant benefit of supporting users' mobility and portable handsets. Ease of deployment and wide coverage make wireless mesh networks (WMNs) very practical for providing VoIP services over wireless networks.

*Corresponding author. E-mail: xuli@fjnu.du.cn, Fax and Tel: 0086-591-83533783.

However, ease of access to the medium makes VoIP over WMNs vulnerable to unauthenticated access and malicious users (Thermos and Takanen, 2008). The vulnerability results from either the characteristics of session initiation protocol (SIP), which has been selected by the major standard committees as the premier protocol for VoIP, or unreliable authentication between mesh nodes. Therefore, while it has become increasingly attractive to deploy VoIP, we still need to understand how VoIP can be deployed over WMNs without placing their information and the continuity of their business at risk. Securing VoIP over WMNs is the first step and a big challenge to provide VoIP service in WMNs widely.

Elbayoumy and Shepherd (2007) presented tiny encryption algorithm (TEA) for securing VoIP. They have proved that TEA has no superior as offering voice traffic confidentiality. Maccari et al. (2006) proposed a fast and secure mobile client re-authentication scheme in WMNs. In their model, a full costly authentication is performed only at the first network entry to speed up the following reauthentication when the client roams to another access point (AP). Frank (2006) demonstrated a hybrid authentication protocol, including mesh node access control by key eraser procedure, topology authentication and communication authentication. Sengar et al. (2006) proposed cross-protocol methods to detect denial-of-service attacks on VoIP. Munir et al. (2010) introduced a new security architecture termed touch me not to avoid signal tapping. In the proposed architecture, a main security master, including a continuous key jumbler which randomly jumble and reassign key values, prevents intruders from key cracking. However the method cannot be generalized in all public sectors as well as private sectors as tapping is restricted in accordance with law. Eun-Jun et al. (2010) revealed the vulnerabilities of both Durlanik and Sogukpinar (2005) and Wu et al. (2009) authentication schemes for SIP to off-line password guessing attacks, Denning-Sacco attacks, and stolen-verifier attacks. To resolve those security issues, Eun-Jun et al. (2010) proposed a new secure and efficient SIP authentication scheme for converged VoIP networks based on elliptic curve cryptosystem (ECC). It has been demonstrated that the proposed SIP authentication scheme resists against those attacks through exploiting the key block size, speed, and security jointly. Ruishan et al. (2010) analyzed several SIP-based VoIP systems and examined how the inherent weaknesses in the SIP and real-time transport protocols (RTP) used by currently deployed VoIP systems. Their experiments showed that millions of subscribers from leading commercial VoIP service providers (for example, Vonage, AT and T and Gizmo) are vulnerable to various billing attacks, that is, the billing of existing SIP-based VoIP services is not trustworthy.

Although the aforementioned methods make some enhancement for WMNs, VoIP and SIP, they consider the security issues of WMNs, VoIP and SIP separately. Furthermore, none of them combines WMNs security with SIP security or VoIP security. So, there are many security issues to be taken into account when we deploy VoIP in a multi-hop WMNs with mutual authentication of intermediate mesh nodes based on SIP. In this paper, we consider security issues for supporting VoIP over WMNs. In particular, we focus on the mutual authentication of intermediate mesh nodes based on SIP.

Security of SIP-based VoIP over WMNs

Figure 1 demonstrates the architecture of session initiation protocol (SIP)-based voice over internet protocol (VoIP) over Wireless mesh networks (WMNs) (Bo et al., 2008), including SIP terminal, SIP proxy server, WMNs and IP core network. Each WMN is connected to the IP core network through a mesh gateway router. Any “internal call” (calls made between clients inside the network), or “external call” (calls made to or from clients outside the network) from a SIP terminal goes through a SIP proxy server. The SIP proxy server is an intermediate device that receives SIP messages from clients and then forwards them to their destination SIP proxy servers through the WMNs. SIP is based on an HTTP-like request/response model and has been specified by the Internet Engineering task Force (IETF) as a standard for signaling and control in multimedia communications over IP (Bo et al., 2008). SIP is used not only to set up a session but also establish a secure communication. As SIP plays an integral role in current and future real time communication networks, protection of SIP networks from different types of attacks is crucial for VoIP security (Sengar et al., 2006; Fadi et al., 2010; Sven Ehlert et al., 2010; Ryu et al., 2009; Yun et al., 2009).

However, it is worth noting that SIP security has the following weaknesses:

- It only applies to a few SIP messages, but leaves other important SIP messages unprotected.
- It only protects a few SIP fields, excludes important SIP fields (for example, SDP, from, to).
- It secures only SIP messages from the user agent client (UAC) to SIP servers.

To address the above issues, the SIP standard, as specified in RFC 3261 (Rosenberg and Schulzrinne, 2002), has proposed several security mechanisms. The SIP specification recommends using transport layer security (TLS) or internet protocol security (IPsec) to protect the SIP signaling path in SIP networks. It suggests using secure/multipurpose internet mail extensions (S/MIME) to protect the integrity and confidentiality of SIP messages. However, it is difficult to protect the SIP messages from end-to-end since intermediate SIP servers need to examine and change certain fields of the SIP messages while they are transmitting through the WMNs.

The openness of a WMN makes it vulnerable to both

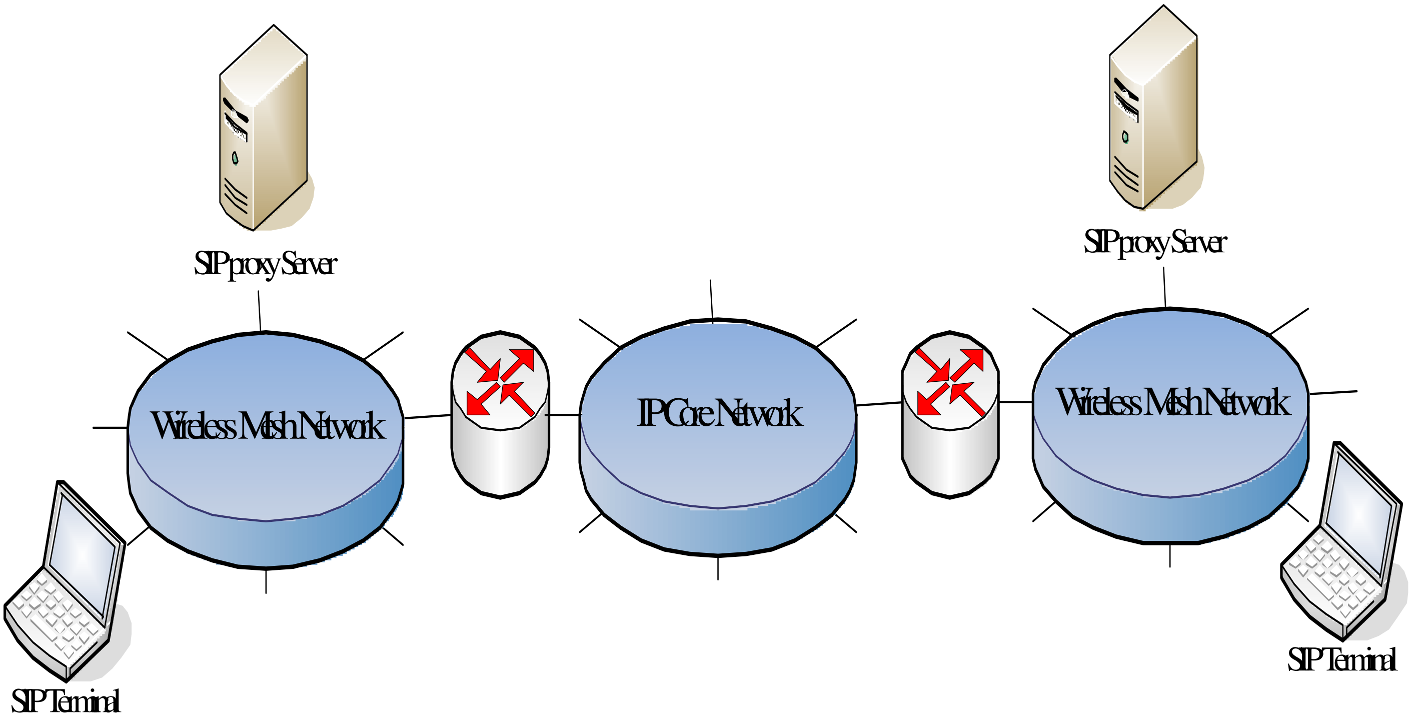

Figure 1. Architecture of SIP based VoIP over WMNs.

external and internal intruders. An external intruder can interrupt the routing by partitioning the network. An inside attacker in the form of a compromised node is much more pernicious as it could attach without being detected. An intruder can make network dysfunction in various ways, for example, route poisoning in the form of generating routing loops and misrouting of data, failing to forward traffic, executing a denial of service (DoS) attack, manipulating the content of payload, or a man-in-the-middle attack. Therefore, the fundamental security primitives of authentication, integrity, and confidentiality are very essential for the correct function of WMNs.

There are two key parameters to secure mesh points (MPs) and mesh clients in WMNs. As the interconnected MPs form the backbone of the network, MPs require the highest level of security. All ongoing traffic should therefore be encrypted using secure standards such as 128- or 256-bit AES encryption, and all MPs and mesh clients should be authenticated in the network. The implementation of encryption and authentication uses standards like 802.11i/EAS/TKIP and authentication servers such as RADIUS and 802.1x, respectively.

These security mechanisms can do some work for WMNs security. However, they are all based on the full trust among nodes in WMNs without considering the betrayal of the authenticated internal nodes. To make the security mechanisms proposed in RFC3261 work efficiently, a pre-call security mechanism between nodes is required.

Subjective logic based dynamic trust mechanism for SIP-based VoIP over WMNs

According to the architecture and security issues mentioned earlier, we propose a subjective logic based dynamic trust mechanism for session initiation protocol (SIP)-based voice over internet protocol (VoIP) over wireless mesh networks (WMNs). We aim at making the detection of malicious mesh nodes more accurate and efficient by overcoming the limitations of existing schemes. In our scheme, we assign weight factor to an opinion according to its expectation, which helps a node obtain a recommended opinion with higher accuracy and reliability. In the proposed mechanism, we have the following premises:

- The wireless links in WMNs are symmetric.
- All the wireless nodes in the networks are equipped with omni-directional antenna and the adjacent nodes are assigned with non-interfering channels.

The details of the subjective logic based dynamic trust mechanism are described next.

Subject logic

Derived from the Dempster-Shafer theory (Shafer, 1976) and with the ability to explicitly represent and manage a node's uncertainty, subjective logic (Josang et al., 2006) has been considered as an attractive algorithm for

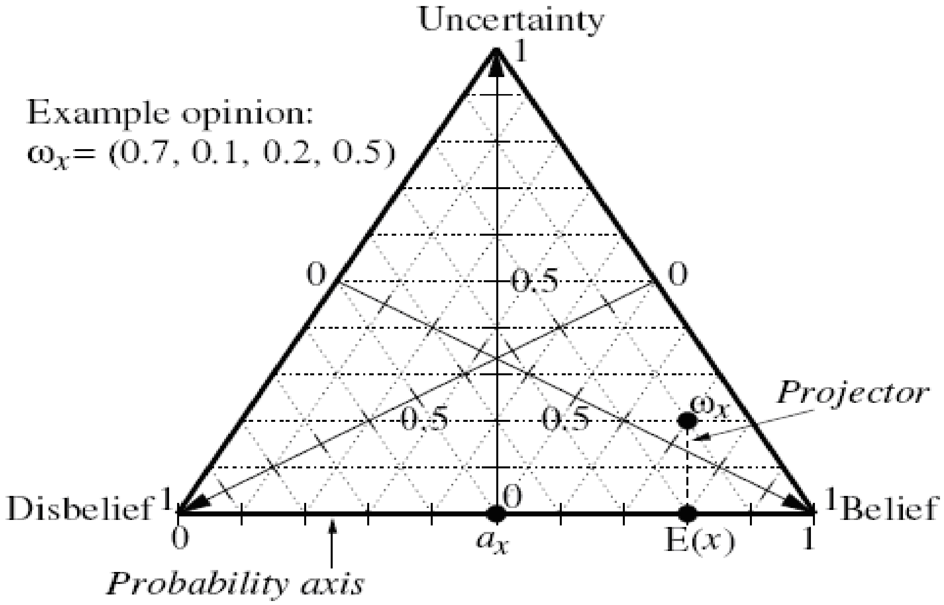

Figure 2. Opinion triangle with example opinion.

handling trust relationships in inherently dynamic, open and uncertain networks. Subjective logic, known as belief calculus, can be indicated by opinion, a belief metric of subjective beliefs. Each opinion is denoted by a 4-tuple $\omega_{x:y} = (b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y})$, where $b_{x:y}$ represents node x's belief in node y, $d_{x:y}$ represents node x's disbelief in node y, $u_{x:y}$ represents node x's uncertainty in node y and $a_{x:y}$ is the base rate. They satisfy the following conditions:

$$\begin{cases} b_{x:y} + d_{x:y} + u_{x:y} = 1.0 \\ b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y} \in [0.0, 1.0] \end{cases} \tag{1}$$

The opinion space can be mapped into the interior of an isosceles triangle, where, for an opinion $\omega_x = (b_x, d_x, u_x, a_x)$, the three parameters b_x, d_x and u_x determine the position of the vertices accordingly. Figure 2 (Kane and Browne, 2006) illustrates an example where the opinion about a proposition x from a binary state space with the value $\omega = (0.7, 0.1, 0.2, 0.5)x$.

Belief and disbelief can be calculated by the collected evidence of uncertainty. The uncertainty reflects the confidence in node x's knowledge on node y; an uncertainty of 1.0 represents that a node has no basis for any conclusions. The base rate, that represents node x's willingness to believe node y, determines how uncertainty is viewed as belief using an opinion. When an opinion is used in a decision, it is projected onto the belief/disbelief axis through its expectation $E(\omega_x) = b_x + a_x u_x$. For a base rate of 0.0, uncertainty is regarded as disbelief, while uncertainty is considered as belief for a base rate of 1.0. When a base rate is 0.5, uncertainty is positively viewed as actual belief. In this paper, we initially use a base rate of 0.5 as uncertainty for each node. Therefore unknown nodes are by default assigned a median level of trust.

For example, if an opinion is (0.6, 0.2, 0.2, 0.5), its expectation can be calculated as $E(\omega_x) = b_x + a_x u_x$ = 0.6 + 0.5 * 0.2 = 0.7. An entirely uncertain opinion, (0.0, 0.0, 1.0, a_x) always has an expectation equal to the base rate, as $E(\omega_x) = b_x + a_x u_x = 0.0 + 1.0 * a_x = a_x$. The base rate then becomes the default opinion for unknown nodes.

Reputation scheme based on subjective logic

The proposed mechanism incorporates uncertainty based on subjective logic in association with the reputation computing. In order to differentiate intentional packet drop from packet drop due to poor link quality, we integrate link quality into the proposed scheme based on subjective logic. The wireless links can have intermediate loss ratios due to their surroundings and inter-flow interference (Saxena et al., 2010). Link quality is measured by probability of successfully transmitting a packet over a wireless link.

For our scheme we use the enterprise archive (EAR)

(Kim and Shin, 2006) for estimating the quality of wireless links by the equation given as:

$$d_i = (1-\alpha)\times d_{i-1} + \alpha \times N_s / N_T \qquad (2)$$

Where: d_i is the smoothed delivery ratio; α is the smoothed constant, $0 < \alpha < 1$; N_s is the number of successful transmissions during the measurement period of the i th cycle; N_T is the total number of transmissions during the measurement period of the i th cycle.

All the calculations for our scheme throughout this paper are performed in time domain.

Direct opinion

In wireless mesh networks (WMNs), for two neighboring nodes x and y, the final opinion of x to y, $\omega_{x:y}^{final}$ includes two components. One is the direct opinion $\omega_{x:y}^{dir}$, the other is the testimonies from other nodes, the recommended opinions $\omega_{x:y}^{rec}$.

The direct opinion of node x to node y $\omega_{x:y}^{dir} = (b_{x:y}^{dir}, d_{x:y}^{dir}, u_{x:y}^{dir}, a_{x:y}^{dir})$ is stored in x' local reputation table. Following the direct interaction history, node x computes $b_{x:y}^{dir}$, $d_{x:y}^{dir}$ and $u_{x:y}^{dir}$. In a measurement period, we let $T_x(y)$ be the total number of packets node x has transmitted to node y for forwarding, $S_x(y)$ denote the number of packets node y has successfully forwarded and $F_x(y)$ be the number of packets node y has not forwarded. The link quality between node x and y, $LQ(x,y)$, can be calculated by Equation 2. Then we have the following equation:

$$\begin{cases} b_{x:y}^{dir} = S_x(y) / (T_x(y) * LQ(x,y)) \\ d_{x:y}^{dir} = F_x(y) / (T_x(y) * LQ(x,y)) \\ u_{x:y}^{dir} = 1.0 - b_{x:y} - d_{x:y} \end{cases} \qquad (3)$$

Each node has its direct opinion on others. For an entirely unknown node or a new node, the default opinion assigned by its neighbors is (0.0, 0.0, 1.0, a).

We classify interactions among nodes into positive, negative and uncertain interactions. Each positive or negative interaction increases the rating of node's knowledge and consequently reduces uncertainty. The parameter $\delta \in [0.0, 1.0]$ determines how much a rating change after an individual interaction between nodes. In the following formulae, we omit the subscript $x:y$ from each opinion 4-tuple. The direct opinions stored in node x 's local reputation table are updated through the following formulae (Yining et al., 2011):

If the interaction is a positive interaction,
If $u \geq \delta$, then

$$\begin{cases} b = b + \delta \\ u = u - \delta \end{cases}$$

Else,

$$\begin{cases} b = b + \delta \\ d = d - (\delta - u) \\ u = 0.0 \end{cases}$$

If the interaction is a negative interaction,
If $u \geq \delta$, then,

$$\begin{cases} d = d + \delta \\ u = u - \delta \end{cases}$$

Else

$$\begin{cases} b = b - (\delta - u) \\ d = d + \delta \\ u = 0.0 \end{cases}$$

If the interaction is an uncertain interaction,
If $b, d \geq \delta / 2$, then,

$$\begin{cases} b = b - \delta / 2 \\ d = d - \delta / 2 \\ u = u + \delta \end{cases}$$

Else if $b < \delta / 2$ and $d \geq \delta / 2$, then,

$$\begin{cases} b = 0.0 \\ d = d - (\delta - b) \\ u = u + \delta \end{cases}$$

Else if $b \geq \delta / 2$ and $d < \delta / 2$, then,

$$\begin{cases} b = b - (\delta - d) \\ d = 0.0 \\ u = u + \delta \end{cases}$$

Else if $b, d < \delta / 2$, then,

$$\begin{cases} b = 0.0 \\ d = 0.0 \\ u = 1.0 \end{cases}$$

This update mechanism ensures that the direct opinion $\omega_{x:y}^{dir} = (b_{x:y}^{dir}, d_{x:y}^{dir}, u_{x:y}^{dir}, a_{x:y}^{dir})$ can be updated in real time by providing a more precise $\omega_{x:y}^{dir}$ for calculation of $\omega_{x:y}^{final}$; meanwhile, with the increasing of the number of interactions, the uncertainty value will decrease to zero. All these can improve the accuracy of isolating untrustworthy nodes.

Recommended opinions

When the direct opinion $\omega_{x:y}^{dir}$ is not enough for node x to make a decision about node y, x solicits the recommended opinions from their common neighbor nodes, the neighbor nodes transmit their direct opinions on y as the recommended opinions to x. Suppose that node x receives a number of subjective opinions as known as recommended opinions. Let R represent the set of recommenders to reflect how much a node's recommended opinion impacts on the reputation computation results, which prevent retaliations or badmouth from occurring after untrustworthy nodes are rejected, we allocate an appropriate weight factor to each recommended opinion. For each recommender $i \in R$, the weight factor f_i is computed as follows:

$$\begin{cases} f_i = E(\omega_{x:i}) \Big/ \sum_{k \in R} E(\omega_{x:k}) \\ E(\omega_{x:i}) = b_{x:i} + a_{x:i} u_{x:i} \end{cases} \qquad (4)$$

Where, $E(\omega_{x:i})$ represents x's belief on i. Since the bigger $E(\omega_{x:i})$ has larger impact on the reputation computation results. The recommended opinion is adopted with higher probability as bigger $E(\omega_{x:i})$. For those untrustworthy nodes, their expectations are very small, so their recommending opinions have little impacts on the reputation computation results,

For recommended opinions, they are given by multiplication of common recommended opinion $\omega_{x:y}^{rec} = (b_{x:y}^{rec}, d_{x:y}^{rec}, u_{x:y}^{rec}, a_{x:y}^{rec})$ and their corresponding weights as follows:

$$\begin{cases} b_{x:y}^{rec} = \sum_{k \in R} f_k \cdot b_{k:y}^{dir} \\ d_{x:y}^{rec} = \sum_{k \in R} f_k \cdot d_{k:y}^{dir} \\ u_{x:y}^{rec} = \sum_{k \in R} f_k \cdot u_{k:y}^{dir} \\ a_{x:y}^{rec} = \sum_{k \in R} f_k \cdot a_{k:y}^{dir} \end{cases} \qquad (5)$$

Final opinion

After getting the direct opinion $\omega_{x:y}^{dir}$ and the recommended opinion $\omega_{x:y}^{rec}$, a final opinion $\omega_{x:y}^{final} = (b_{x:y}^{final}, d_{x:y}^{final}, u_{x:y}^{final}, a_{x:y}^{final})$ is calculated by (Yining, et al., 2011):

$$\begin{cases} b_{x:y}^{final} = \left(b_{x:y}^{dir} \cdot u_{x:y}^{rec} + b_{x:y}^{rec} \cdot u_{x:y}^{dir}\right) \Big/ \left(u_{x:y}^{dir} + u_{x:y}^{rec} - u_{x:y}^{dir} \cdot u_{x:y}^{rec}\right) \\ d_{x:y}^{final} = \left(d_{x:y}^{dir} \cdot u_{x:y}^{rec} + d_{x:y}^{rec} \cdot u_{x:y}^{dir}\right) \Big/ \left(u_{x:y}^{dir} + u_{x:y}^{rec} - u_{x:y}^{dir} \cdot u_{x:y}^{rec}\right) \\ u_{x:y}^{final} = \left(u_{x:y}^{dir} \cdot u_{x:y}^{rec}\right) \Big/ \left(u_{x:y}^{dir} + u_{x:y}^{rec} - u_{x:y}^{dir} \cdot u_{x:y}^{rec}\right) \\ a_{x:y}^{final} = a \end{cases} \qquad (6)$$

When both the direct opinion $\omega_{x:y}^{dir}$ and the recommended opinion $\omega_{x:y}^{rec}$ are determined, and the denominator $(u_{x:y}^{dir} + u_{x:y}^{rec} - u_{x:y}^{dir} \cdot u_{x:y}^{rec})$ in Equation 6 is zero, we take the limit and compute the final opinion $\omega_{x:y}^{final}$:

$$\begin{cases} b_{x:y}^{final} = \beta \cdot b_{x:y}^{dir} + (1 - \beta) \cdot b_{x:y}^{rec} \\ d_{x:y}^{final} = \beta \cdot d_{x:y}^{dir} + (1 - \beta) \cdot d_{x:y}^{rec} \\ u_{x:y}^{final} = 0 \\ a_{x:y}^{final} = a \end{cases} \qquad (7)$$

Where, β is a weight, which determines how much the direct opinion $\omega_{x:y}^{dir}$ impacts on the final opinion $\omega_{x:y}^{final}$.

Decision procedure

There are two types of wireless mesh nodes in wireless mesh networks (WMNs), cooperative nodes and malicious nodes. The former carries out operations faithfully, while the latter is interested in making use of the network with a minimal expense or doing malicious attacks. Therefore, when a node y requests for some services from its neighbor node x, x has to carry out a decision procedure to identify y's intention. Let $\gamma \in [0.0, 1.0]$ be a threshold, if the expectation $E(\omega_{x:y})$ is larger than γ, y will be perceived as a cooperative and trustworthy node and the services requested will be granted by x. The decision procedure is as follows:

1. Node y sends a Path_Request message to one of its neighbor nodes x.
2. After receiving Path_Request successfully, x performs different algorithms according to its type. If x is a trustworthy node, it performs algorithm (I); if x is an untrustworthy node, it performs algorithm (II).

Algorithm (I)

(1) X retrieves its direct opinion $\omega_{x:y}^{dir}$ from its local reputation table and calculates the expectation $E(\omega_{x:y}^{dir})$.

(2) If $E(\omega_{x:y}^{dir}) \geq \gamma$, x sends an accept message to y and provides the requested service, and y records a positive interaction with x; else, x invokes the reputation query procedure.

(a) X broadcasts a Reputation_Query to the common neighbor nodes with y for the recommending opinions on y and waits for a time interval T.

(b) Any node k whose uncertainty $u_{k:y}^{dir}$ of its direct opinion is less than 1.0 sends its direct opinion $\omega_{k:y}^{dir}$ to x.

(c) After the time interval T, x weighs each received recommended opinions using Equation 4, integrates them into a recommended opinion $\omega_{x:y}^{rec}$ using Equation 5, and combines the direct opinion $\omega_{x:y}^{dir}$ with the recommended opinion $\omega_{x:y}^{rec}$ using Equations 6 or 7. Finally, x obtains the final opinion $\omega_{x:y}^{final}$.

(d) After obtaining the final opinion $\omega_{x:y}^{final}$, x calculates its expectation $E(\omega_{x:y}^{final})$. If $E(\omega_{x:y}^{final}) \geq \gamma$, x sends an Accept message to y and provides the requested service, and y records a positive interaction with x; else, x sends a Refuse message to y, and y records a negative interaction with x.

Algorithm (II)

(1) Let $\theta \in [0.0,1.0]$ be the probability that an untrustworthy node cooperates in an attempt to hide its untrustworthy intent. When x receives a request message from y, then x flips a coin weighted by probability θ.

(a) If the coin flip indicates to cooperate, x sends an accept message to y and provides the requested service, and y records a positive interaction with x.

(b) If the coin flip indicates not to cooperate, x refuses to provide service to y, and y records a negative interaction with x.

If the expectation of a node k $E(\omega_k) < \gamma$, node k is perceived as an untrustworthy node. It is temporarily excluded from the network so that it can be forced to cooperate and put into a probation state. The probation period is initially T, which is the same as the period of reputation query. At the end of T, k is given another chance to calculate its expectation $E(\omega_k)$, if $E(\omega_k)$ is still less than γ, then k is put into another probation state for a longer period (2T). Therefore, the probation period of an untrustworthy node is doubled on every subsequent offence until it reaches a maximum value $T_{\max}$, then it is permanently excluded from the network.

So far, the overall workflow of our proposed scheme is completed. Untrustworthy wireless mesh nodes in WMNs are detected and isolated through the above-mentioned scheme.

Performance analysis

In this section we validate our mechanism in NS2 using the session initiation protocol (SIP) extension defined by the internet engineering task force (IETF). The SIP extension allows a user agent to convey its capabilities and characteristics to other user agents and servers (Shafer, 1976).

We implement the simulation by adding two new parameters and , indicating “trustworthy interaction” and “non-trustworthy interaction”, respectively into contact header filed of the REGISTER message. The values of And are integers and completely implementation dependent. For example, a SIP terminal fills the following contact header of the REGISTER message as: Contact :< sip : hawk @ 192.168.1.2 >; ci = 0"; nci = ”0”. With the parameters “from”, “to”, “contact ci nci”, we can identify the information carried by this REGISTER message direct or indirect, also trustworthy or not.

Therefore the resistance to identity attacks is important for wireless mesh networks (WMNs) security, we compare the performance of identity attacks and defense between traditional cryptography-based authentication mechanisms and our subjective logic based dynamic trust mechanism.

Simulation settings

The simulation scenario is defined in an area of 1000 * 1000 m with 50 wireless mesh nodes randomly deployed. Each node is equipped with an omni-directional antenna with direct radio transmission range of 250 m. The simulation time is 100 s and each node randomly selects one of its neighbors and requests services every 5 s. The WLAN MAC layer uses the distributed coordination function (DCF) of Institute of Electrical and Electronics Engineers (IEEE) 802.11 and the routing protocol is ad hoc on demand distance vector (AODV). The simulation environment setting parameters are shown in Table 1.

Performance metrics

To evaluate the performance of the proposed scheme, we consider the following metrics:

1. Rates of the malicious nodes identification- the ratio to identify the malicious nodes. It is desirable for this ratio to be as high as possible.
2. Packet delivery rate (PDR) - the ratio of total number of packets that have been received by destination to the total number of packets sent by the source. It shows how effectively the network transmits packets from source to destination. It is desirable for this ratio to be as high as possible.
3. False positive rate - the percentage of number of trustworthy nodes wrongly detected as malicious out of the total number of trustworthy nodes in the network. It is desirable for this rate to be as small as possible.

Simulation results

Scenario 1

In scenario 1, we first simulate a network with 70% of the nodes malicious to set a hostile network environment. In addition, nodes in the network do not know each other at the beginning and no packet is dropped due to network ambiguities. Secondly, we let 30% of nodes in the network

Table 1. Simulation environment and parameters setting.

Parameter	Value
Traffic type	CBR
Simulation area	1000 m * 1000 m
Packet rate	2 packets /s
Total number of wireless nodes	50
Simulation Time	100s
Packet size	1024 bytes
Maximum mobility velocity (Vmax)	2 m/s
Base rate a	0.5
Variation δ	0.1
Weight factor β	0.5
θ	0.3
Threshold γ	0.6
Reputation query period T	5 s
Isolation time Tmax	20 s

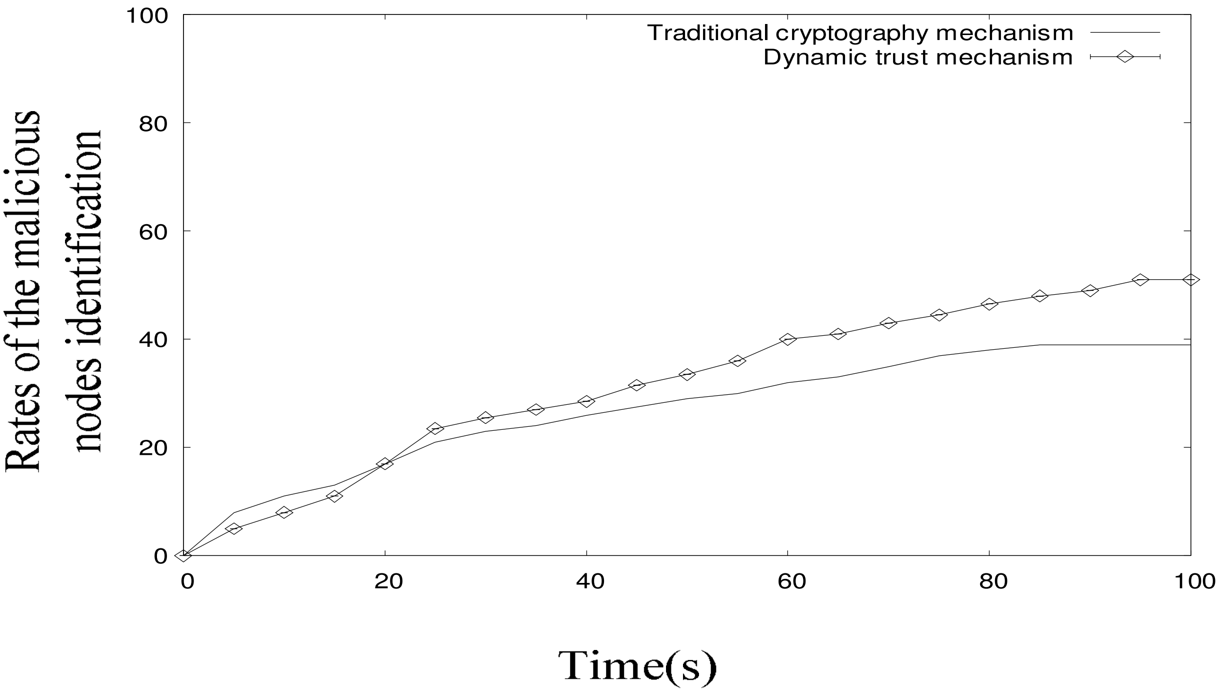

Figure 3. Rates of the malicious nodes identification dataset scale in a hostile network.

be malicious. The success of building a sufficient trust relationship out of attempts is around 70%, as same as the percentage of honest nodes in the network. The simulation results of scenario 1 are shown in Figures 3 and 4, respectively.

As shown in the Figures 3 and 4, it takes nodes around 20 s to build up the trust relationships among them from the beginning until knowing each other. Therefore in the first 20 s, the traditional mechanism is better than the proposed mechanism in terms of malicious nodes identification rate. With the growth of running time, the trust relationships of nodes have been built up, the proposed dynamic mechanism is superior to traditional cryptography-based authentication mechanism in identifying the malicious nodes, especially in the hostile network. The results showed that our model can enhance the security of the session initiation protocol (SIP-based) voice over internet protocol (VoIP) over wireless mesh

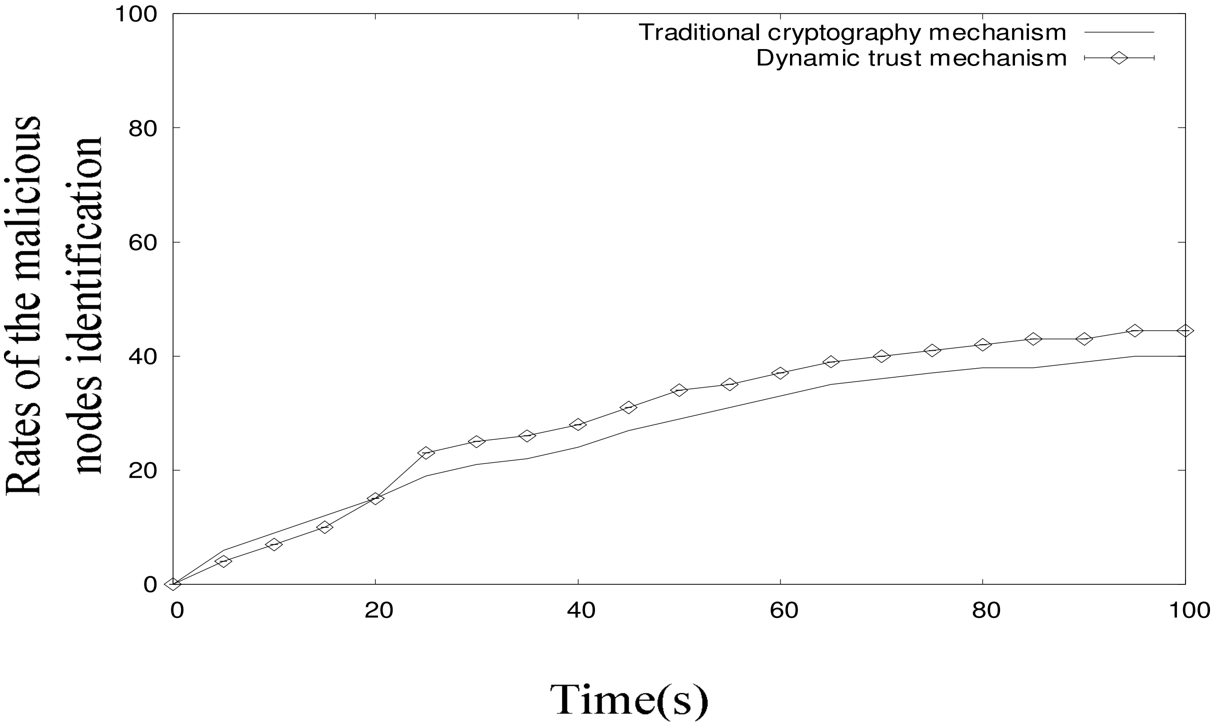

Figure 4. Rates of the malicious nodes identification dataset scale in an honest network.

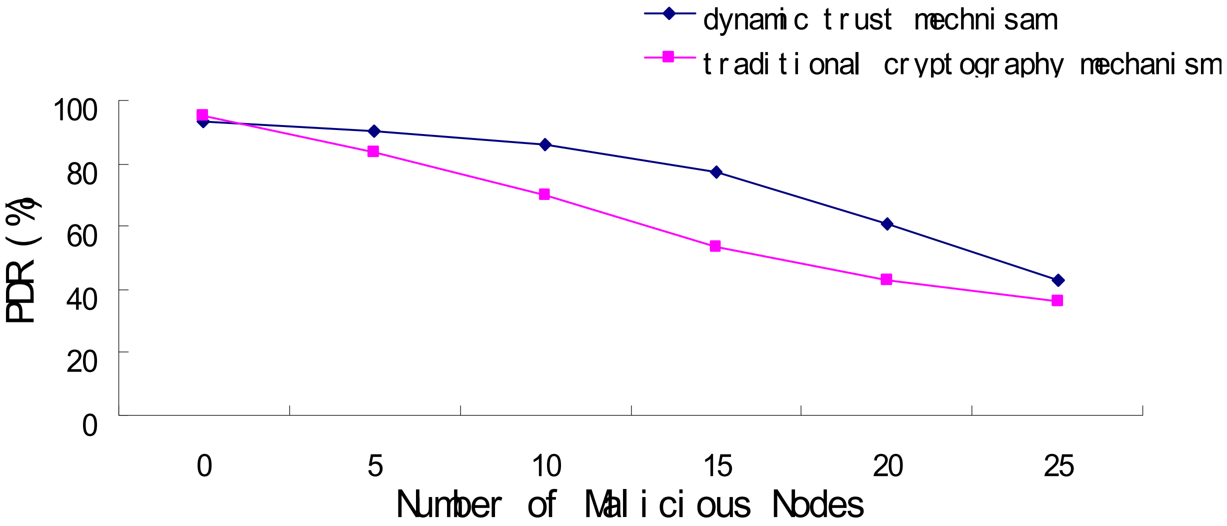

Figure 5. PDR comparison.

networks (WMNs) more efficiently.

Scenario 2

In this scenario, we investigate the effectiveness of detecting malicious nodes by measuring the packet delivery rate (PDR) under various network conditions as a function of the number of malicious nodes. As shown in Figure 5, the performance of network decreases as the number of malicious nodes increases. When there is no malicious node in the network, the PDR of the proposed scheme is slightly lower than the traditional mechanism due to detection overhead. As the number of malicious nodes increases, both performances of the two schemes decrease, while the performance of traditional mechanism

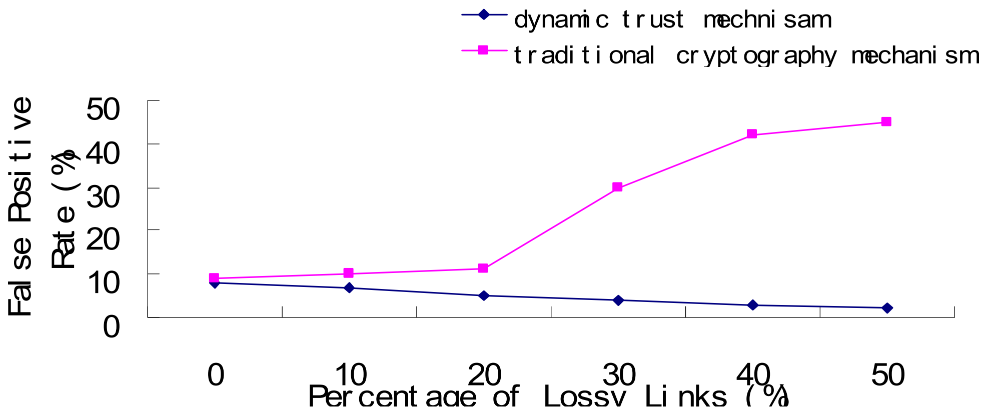

Figure 6. Comparison of false positive rate as a function of link quality.

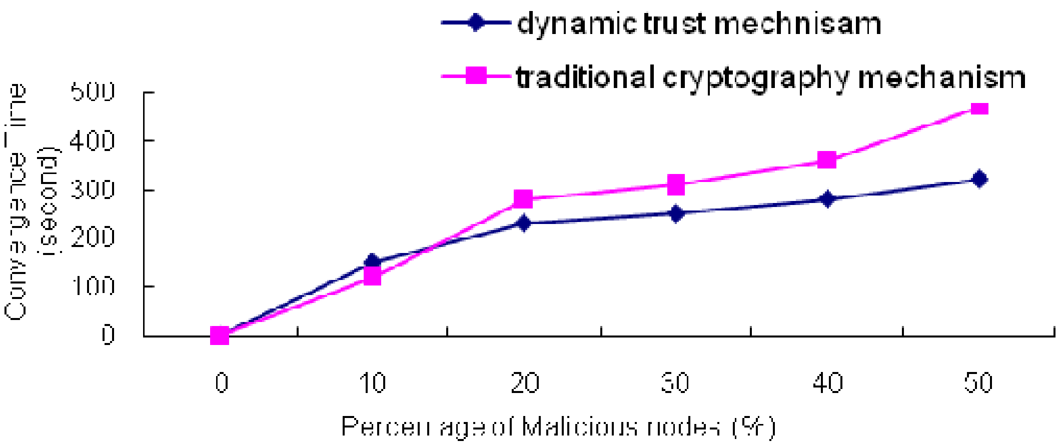

Figure 7. Comparison of convergent time.

decreases faster than the proposed scheme. It is worthy of note that when the number of malicious nodes is over 15, the performance of the proposed scheme declines rapidly and get close to the traditional mechanism. The reason behind this is that when the ratio of malicious nodes is higher, there are fewer alternatives available for selecting forward paths, and malicious nodes may be included in the forward paths.

Scenario 3

In this scenario, we turn to evaluate the effect of poor quality links on performance. The poor quality links are simulated by setting forward ratio range from 0.4 to 0.6. We vary the number of lossy wireless links and examine the number of false positives given by the proposed scheme and the traditional cryptography-based authentication mechanism. The simulation results are shown in Figure 6. The proposed mechanism does show a few false positives for lower percentage of lossy links. These false positives result from the packet loss caused by poor link quality. Since the traditional mechanism does not have a function of differentiating intentional packet drop from packet drop due to link quality, packets loss due to link quality is falsely detected as malicious behavior. Different from the traditional mechanism, the proposed scheme has the function. Therefore, as the number of lossy links increases, the false positive rate of traditional mechanism raises, while the false positive rate of the proposed scheme decreases.

To validate the effectiveness of the proposed scheme, we also measure the convergence time between the proposed scheme and the traditional cryptography-based authentication mechanism. Figure 7 depicts the convergence time of the two schemes against varying percentage of malicious nodes. The parameter is set to 0.3 so malicious nodes can hide their malicious behaviors to a certain degree. As shown in Figure 7, convergence times of the two schemes go up as the percentage of malicious nodes increases, and convergence time of the proposed scheme is less than the traditional cryptography-based authentication mechanism. Along with a growing percentage of malicious nodes, the more malicious nodes are isolated, subsequently the more forward routings are broken, and the less reliable information for calculating the reputation values is. Thus, cooperative nodes have to spend more and more time identifying other malicious nodes. By applying weight factor and the reconfirmation scheme of malicious nodes, the proposed scheme can calculate reputation values and isolate malicious nodes more accurately and effectively, and its convergence time improves significantly.

Conclusion

WMNs are considered as an alternative to traditional wired broadband access. Thus, existing broadband applications such as VoIP and video conferencing are expected to work well on the WMNs with few or no modifications. However, security provisioning in VoIP over WMNs is a very challenging issue due to inherent characteristics of WMNs such as dynamical changing of topology, wireless and multi-hop communications, etc. Although many methods have reinforced WMNs, VoIP and SIP, they consider the security issues of WMNs, VoIP and SIP, separately.

To fill the gap of combination WMNs with SIP security, we consider security issues for supporting VoIP over WMNs and propose a subjective logic-based dynamic trust mechanism in this paper. In particular, we focus on the mutual authentication of intermediate mesh nodes based on SIP. By validating the performance of the proposed dynamic trust model through network simulator 2 (NS2), we prove that the proposed model provides a more practical solution for enhancing the security of SIP-based VoIP over WMNs.

ACKNOWLEDGMENT

This work is supported partially by National Natural Science Foundation of China with grant NO.61072080 and the Education Department of Fujian Province with grant NO. JA09046.

ABBREVIATIONS

VoIP, Voice over internet protocol; **WMNs**, wireless mesh networks; **SIP**, session initiation protocol; **NS2**, network simulator 2; **POTS**, plain old telephone system; PSTN, public switched telephone network; **TEA**, tiny encryption algorithm; **AP**, access point; **ECC**, elliptic curve cryptosystem; **UAC**, user agent client; **TLS**, transport layer security; **IPse**c, internet protocol security; **S/MIME**, secure/multipurpose internet mail extensions; **MPs**, mesh points; **IETF**, Internet Engineering Task Force; **DCF**, distributed coordination function; **IEEE**, Institute of Electrical and Electronics Engineers; **AODV**, ad hoc on demand distance vector; **PDR**, packet delivery rate, **RTP** real-time transport.

REFERENCES

Barnard P (2009). Gartner: More than 50% of Mobile Voice Traffic will be VoIP by 2019. http://www.fiercevoip.com/story/gartner-more-50-mobile-voice-traffic-will-be-voip-2019/2009-05-06.

Barnard P (2009). ABI Study Predicts 267 Million Residential VoIP Subscribers Worldwide by 2012. http://www.tmcnet.com/voip/ip-communications/articles/4824-abi-study-predicts-267-millionresidential-voip-subscribers.htm.

Bo R, Yi Q, Hsiao-Hwa C (2008). An Enhanced SIP Proxy Server for Wireless VoIP in Wireless Mesh Networks. IEEE Commun. Mag., 46(1): 108-113.

Durlanik A, Sogukpinar I (2005). SIP authentication scheme using ECDH. World Enformatika Society Trans. Eng. Comput. Technol., 8: 350-353.

Elbayoumy AD, Shepherd.S (2007). A Comprehensive Secure VoIP Solution. Int. J. Netw. Secur., 5(2): 233-240.

Enterprise (2009). VoIP Adoption. http://www.voip-news.com/press-releases/enterprise-adoption-america-forecast-projection-021407/

Eun-Jun Y, Kee-Young Y, Cheonshik K, You-Sik H, Minho J, Hsiao-Hwa C (2010). A secure and efficient SIP authentication scheme for converged VoIP networks. Comput. Commun., 33, 1674-1681.

Fadi E, Parmindher M, Andy J (2010). Overview of SIP Attacks and Countermeasures. Info. Secur. Dig. Forensics, 41: 82-91.

Frank R (2006). Authentication in Wireless Mesh Networks. Master Thesis, Universite Joseph Fourier, Grenoble, France.

Higdon J (June 2009). 25 Most Interesting VoIP Startups. http://www.voip-news.com/feature/25-most-interesting-voip-startups-021207.

Josang A, Gray E, Kinateder M (2006). Simplification and Analysis of Transitive Trust Networks. Web Intell. Agent Syst. J., 4(2): 139-161.

Kane P, Browne PC (2006). Using uncertainty in reputation methods to enforce cooperation in ad-hoc networks. WiSe2006, Los Angeles, USA , pp. 105-113.

Kim K, Shin KG (2006). On Accurate Measurement of Link Quality in Multi-Hop Wireless Mesh Networks. In Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, MOBICOM 2006. Los Angeles, California , USA, pp. 38-49.

Yining L, Keqiu L, Yingwei J, Yong Z, Wenyu Q (2011). A novel reputation computation model based on subjective logic for mobile ad hoc networks. Future Generation Computer Systems, 27(5): 547-554. (2011). A novel reputation computation model based on subjective logic for mobile ad hoc networks. Fut. Gen. Comput. Syst., 27(5): 547-554.

Maccari L, Fantacci R, Pecorella T (2006). Secure, fast handhoff techniques for 802.1X based wireless network. In Proceedings of IEEE ICC. Istanbul TURKEY, pp. 3917 - 3922,

Munir B, Sayyad A Chatterjee S, Nalbalwar L (2010). Proposed Model for SIP Security Enhancement. Communication and Network, 2: 69-72.

Perez M (2009). Report: Cable VoIP Market. http://www.voipnews.com/news/cable-voip-market-report-080406/

Perez M (2009). VoIP Service Providers Residential. http://www.voip-info.org/wiki/view/VOIP+Service+Providers/

Rosenberg J, Schulzrinne H (2002). SIP: session initiation protocol. RFC 3261.

Ruishan Z , Xinyuan W , Xiaohui Y, Xuxian J (2010). On the billing vulnerabilities of SIP-based VoIP systems. Computer Networks, 54: 1837-1847

Ryu JT, Roh BH, Ryu KY (2009). Detection of SIP Flooding Attacks Based on The Upper Bound of The Possible Number of SIP Messages, KSII Transactions Internet Info. Syst., 3(5): 507-526.

Saxena N, Denkol M, Banerji D (2010). A Hierarchical Architecture for Detecting Selfish Behavior in Community Wireless Mesh Networks. Computer Communications. doi:10.1016/j.comcom.2010.04.040.

Sengar H, Wijesekera, D, Wang H, Jajodia S (2006). VoIP Intrusion Detection Through Interacting Protocol State Machines. In Proceeding of the International Conference on Dependable Systems and Networks. Philadelphia, Pennsylvania USA, pp. 393-402.

Sengar H, Wijesekera, D, Wang H, Jajodia, S (2006). VoIP Intrusion Detection Through Interacting Protocol State Machines. In Proceeding of the International Conference on Dependable Systems and Networks. Philadelphia, Pennsylvania, USA, pp. 393-402.

Shafer G (1976). A Mathematical Theory of Evidence. Princeton University Press, Princeton, NJ.

Sven E , Dimitris G, Thomas M (2010). Survey of Network Security Systems to Counter SIP-based Denial-of-Service Attacks. Comput. Secur., 2 9: 243- 225

Thermos P, Takanen, A (2008). Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures. Addison Wesley, London ,UK.

Wu L, Zhang Y, Wang F (2009). A new provably secure authentication and key agreement protocol for SIP using ECC. Computer Standards and Interfaces, 31(2): 286-291.

Yun HN, Hong SC, Lee,HW (2009). Stateful virtual proxy for sip message flooding attack detection. KSII Trans Intern. Inf. Syst., 3(3): 251-265.