A new trusted roaming protocol in wireless mesh networks

Peng Xiao*

College of Computer Science and Technology,
Beijing University of Technology,
Beijing 100124, China
Email: xp4523@emails.bjut.edu.cn
*Corresponding author

Jingsha He and Yunli Chen

School of Software Engineering,
Beijing University of Technology,
Beijing 100124, China
Email: jhe@bjut.edu.cn
Email: yunlichen@bjut.edu.cn

Yingfang Fu

Fantai Lingshi Technology (Beijing) Limited,
Beijing 100044, China
Email: fuyingfang@bjut.edu.cn

Abstract: Wireless Mesh Networks (WMNs) are a wireless broadband access technology based completely on IP technologies and has thus rapidly become a means for broadband access with the characteristics of high capacity, high speed and wide coverage. For trusted roaming in WMNs, the configuration of the access platforms must be checked first before access to the network can continue, and only those platforms whose configurations meet the security requirements of the network can be allowed to access the network. It is also required that mobile nodes complete access authentication not only in a timely manner, but also in a way in which the identities of the mobile nodes are well protected. In this paper, we propose a trusted roaming protocol that are based on several technologies such as hierarchical network model, elliptic curve cryptography (ECC), trust evaluation, grey relevance analysis, etc. to ensure the security of roaming in WMNs. We also show the security properties of the proposed protocol through formal analysis and the performance by presenting some simulation results.

Keywords: WMN; wireless mesh networks; security; trusted computing; roaming; trusted network connect.

Reference to this paper should be made as follows: Xiao, P., He, J., Chen, Y. and Fu, Y. (2013) 'A new trusted roaming protocol in wireless mesh networks', *Int. J. Sensor Networks*, Vol. 14, No. 2, pp.109–119.

Biographical notes: Peng Xiao is currently a PhD candidate in the College of Computer Science and Technology at Beijing University of Technology. His research interests include network security, trusted authentication in WMNs and Ad Hoc networks.

Jingsha He is currently a Professor of the School of Software Engineering at Beijing University of Technology. His research interests include network security and wireless communication technologies.

Yunli Chen is currently a Professor of the School of Software Engineering at Beijing University of Technology. Her research interests include QoS improvement and wireless mesh networks.

Yingfang Fu is currently a researcher in Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China. Her research interests include network security and trusted computing in WMNs.

1 Introduction

Wireless mesh networks are a new technology of wireless networks that are designed to overcome the limitations of Ad Hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs) and wireless metropolitan area networks (WMANs). Thus, WMNs can be used to build commercial wireless mobile networks to offer services with guaranteed quality. Combining the advantages of WLANs and Ad Hoc networks, WMNs are a wireless broadband access technology based completely on IP technologies and has thus become an effective broadband access means with the characteristics of high capacity, high speed and wide coverage. To some extent, WMNs are mainly a network design approach in which there is no central administration and the network possesses the properties of self-organisation, multi-hop and best routing judgment (Gamer et al., 2011). Since WMNs don't rely on fixed infrastructure and are operated in an open space, any users within the coverage area of the radio waves can access the networks. Therefore, access authentication becomes imperative in preventing unauthorised users from accessing the network (Yi et al., 2009; Cesana et al., 2011). For secure roaming in WMNs, it is further required that mobile nodes complete access authentication not only in a timely manner, but also in a way in which the identities of mobile nodes are effectively protected.

Past practice in information security has shown that most security problems come not just from the network but more from terminal nodes (Khan et al., 2008a; Khan et al., 2008b). The original idea of trusted computing was thus proposed to ensure the security of network terminals. Trusted computing is a means to guarantee the security of a whole computer system in which a root of trust is first built in order to construct a chain of trust, from the root to the hardware platform, to the operation system, and finally to the applications. Thus, trust can be expanded to a whole computer system through graded authentication as well as establishment of trust. For secure roaming in WMNs, the configurations of platforms must be checked first before access to the network can continue and only those platforms whose configurations meet the security requirements of the networks can be allowed to access the networks. This helps to ensure that a terminal with potential threat cannot access the networks directly. At the same time, the terminal node can verify the security of the access point (AP) and would only connect to a network that satisfies its own security requirements (Munoz and Mana, 2010).

Based on the current 802.1x authentication scheme and trusted computing technologies, we propose in this paper a trusted roaming protocol to ensure the security and trust in a WMN. After presenting the protocol, we will show the security properties of the protocol through formal analysis and the performance through simulations.

The rest of this paper is organised as follows. In Section 2, we review some related work on trust establishment and roaming protocols in WMNs. In Section 3, we present a zone-based hierarchical network model for hybrid WMNs, which is the foundation of our protocol. In Section 4, we describe the method for evaluating the trust of both the starting and the runtime states in a trusted system. In Section 5, we present our roaming protocol, which is based on several technology such as hierarchical network model, ECC, trust evaluation, grey relevance analysis, etc. In Section 6, we perform a formal analysis on the proposed protocol based on the strand space model to prove its security properties and, in Section 7, we present some simulation results to show the performance. Finally, in Section 8, we conclude this paper in which we also describe our future work.

2 Related work

Chen proposed a dynamic trust model based on time frames to support the change of dynamic behaviour in the nodes as well as effective information syndication in the network (Chen and Gui, 2007). In his model, recent trust, long-term trust, accumulative abused trust, and feedback trust are introduced to evaluate the trust of nodes. However, since the trust of a node relies on the assessment and feedback by some other nodes, this model has the drawbacks of subjectivity and uncertainty.

Wang proposed a behaviour analysis based dynamic trust measurement model, applying the method of describing program behaviour through the control flow graph for dynamic trust measurement (Wang et al., 2011). The model first measures the program before it is loaded, then generates the expected behaviour model for the program according to static analysis. Then, the model monitors the program's execution in real time by checking the flow branches of the program against the expected behaviour model. However, the expected behaviour sometimes cannot be attained and measured, thus trust measurement and evaluation cannot be successfully carried out.

IEEE P802.11s™/D1.01 (IEEE, 2007) provides an EMSA (Efficient Mesh Security Association) authentication scheme based on the IEEE 802.11i standard, in which the 802.1x scheme and four handshakes are adopted to implement access authentication and key establishment. EMSA makes use of EAP (Extended Authentication Protocol) as EAP-SIM, EAP-TLS, EAP-TTLS, and PEAP, etc. However, roaming in WMNs isn't adequately addressed in EMSA since EMSA cannot meet the requirements of performance as well as identity protection in roaming.

Yang proposed a new mesh roaming access protocol based on DH key agreement, which is called EAP-MRAP (Yang et al., 2008). In the protocol, a mobile node encrypts its identity with HA's (Home Agent) public key in order to hide and protect its identity. Then, a DH key exchange is carried out to ensure the security of the session key agreement. In this scheme, it is assumed that there exists a secure channel between FA (Foreign Agent) and HA, so a necessary authentication of FA is missing. Moreover, since the master key KS exists directly in the network when it propagates from the HA to the FA, it can be easily attacked.

Ma et al. proposed an efficient authentication protocol for WLAN mesh networks in the trusted environment, which is called TWMAP (Ma et al., 2010). In his scheme, it is assumed that PDP (Policy Decision Point), the network controller and service provider in WLAN, is a credible entity which responds to the access request honestly. Since his scheme lacks a mutual authentication to authenticate the PDP, it can only be useful in a WLAN-based WMN. In a no-centre, self-organised WMN, mutual authentication is necessary to prove the identity of every all node. But in his scheme, the *plat_ver_msg* message is transmitted in a plaintext form, thus can be tampered with or defalcated by a man-in-the–middle attack.

Du et al. proposed a cryptography based key management scheme for heterogeneous sensor networks (Du et al., 2009). In his paper, a heterogeneous sensor network (HSN) model is designed for better performance and security, and ECDH is used to accomplish key agreement. Its main advantage is the routing-driven scheme, which only establishes shared keys for those neighbour sensors who communicate in the route. But in most multi-hops environment, the route is changed anytime by the network situation, and there is no fixed route in WMNs, then routing-driven is not so appropriate. Group key is more useful in WMNs.

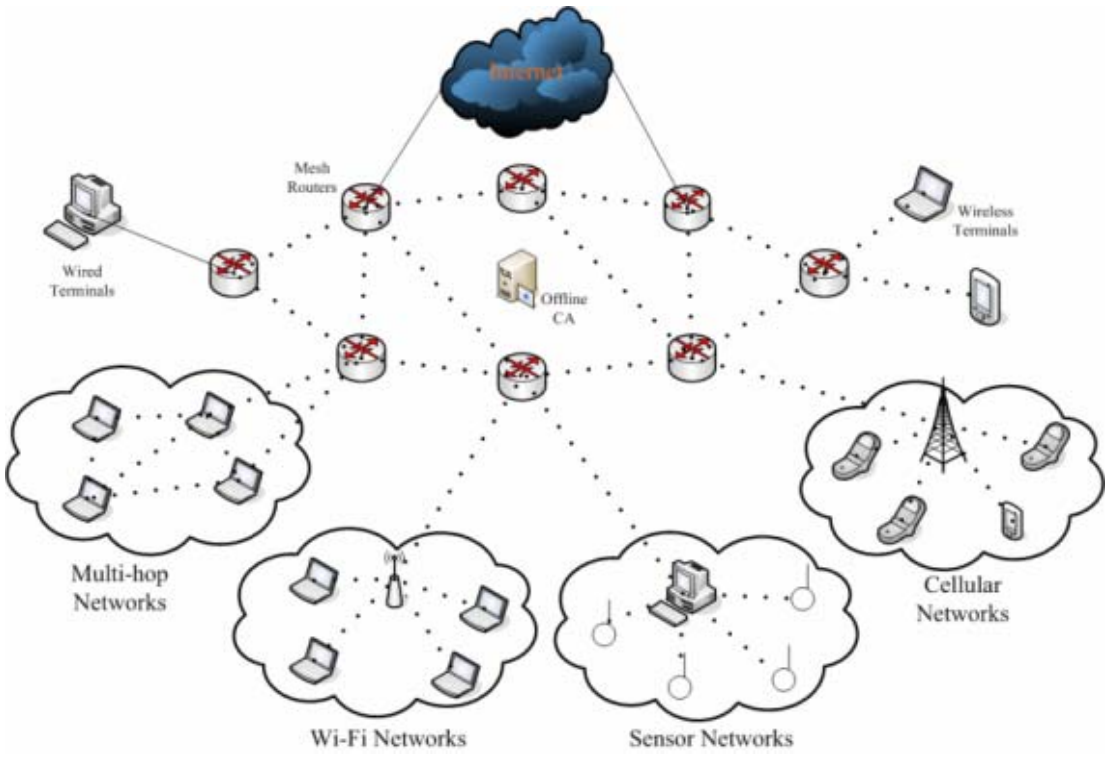
ECC is a permute cryptography in network security. Since it offers equivalent level of security but with smaller key sizes and faster computation speed compared to some other schemes such as RSA, it is involved in many key management schemes, such as ECDH, ECDSA (Du et al., 2009; Wang et al., 2006). Finnigin et al. (2007) analysed the disadvantage of ECC by launching a brute-force attack on an elliptic curve cryptosystem implemented on UC Berkley's TinyOS operating system for wireless sensor networks. His result shows that most ECC can be deciphered in limited computation time. However, Pseudorandom Number Generator (PRNG) is used in his experiment to generate random numbers, but in our paper the random integers are generated by the hardware TPM, which provides better random performance and much more security.

3 Roaming model in hierarchical WMN

A zone-based hierarchical network model for hybrid WMNs is shown in Figure 1, in which dash and solid lines indicate wireless and wired links, respectively (Akyildiz and Wang, 2005; Benyamina et al., 2012). The whole network consists of one backbone network, one or more local area networks called zones and some scattered wired or wireless terminals.

In the backbone network, the mesh routers form a mesh infrastructure with self-configuring, self-healing and self-organising links among which there are at least two backbone routers connected to the Internet. All backbone routers share a single database storing authorised certificates that is not explicitly shown in the figure. There is an offline CA (Certificate Authority) supported by an ISP (Internet Service Provider) or a network carrier. The CA connects to the network only when it is notified of the existence of a new terminal user, a new zone router or a new backbone router. The backbone network can be built using various types of radio technologies including the IEEE 802.11 technologies.

Figure 1 Network model (see online version for colours)



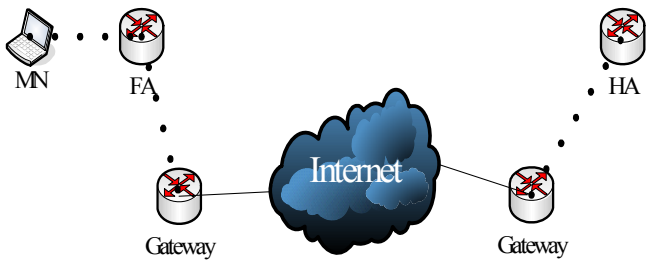
Zones are connected to the backbone network through border mesh routers called gateways, which enables the integration of existing wireless networks, such as multi-hop networks, Wi-Fi networks, sensor networks, cellular networks, etc. In each zone, there is at least one mobile node called AP (Access Point) that is connected to the backbone, such as MAPs (Mesh Access Point) in multi-hop networks and microwave towers in cellular networks. APs may use different radio technologies. It is therefore required that the backbone border routers support various radio technologies. There is also a database that stores user information, such as user ID, zone ID, authorised key, etc. in each zone. Terminal nodes can roam from one zone to another or hand off from one AP to another in the same or different zones.

Conventional terminals with an Ethernet interface can be connected to mesh routers via Ethernet links, whether wired or wireless. For conventional terminals with the same radio technologies as mesh routers, they can directly communicate with the mesh routers. If different radio technologies are used, terminals must communicate with a zone's AP that has Ethernet connections to the mesh routers. Especially, mesh terminals can access the network through mesh routers or directly meshing with other mesh terminals in multi-hop networks whose routing capabilities can provide improved connectivity and coverage.

When a user wants to access a trusted WMN, the network administrator needs to measure its platform configuration information, and compare the measured value with some reference values of the network to verify its security under the current network security policies (Zhang et al., 2010).

Many entities are involved when roaming is considered in this paper, including MN (Mobile Node), FA, HA, Gateway and the Internet, as shown in Figure 2. With the framework of the network model depicted in Figure 1, MN, FA and HA are located in a zone network while Gateway is located in the backbone network. It is assumed that a predefined security association already exists between MN and HA, i.e., MN knows HA's public key while correspondingly HA knows MN's identity, certificate or secret key; MN and HA both know the home zone network's security parameters, FA and HA can get each other's public-key certificate (Xiao et al., 2012).

Figure 2 Roaming mode (see online version for colours)



4 Trust establishment

Integrity measurement is one of the basic mechanisms to establish the trust of a system. The basic concept is that any entity which wants to gain the control must be trust-measured and integrity-validated, including hardware, operating system, shared libraries, configuration documents, and so on. From the power supplying of the platform to the establishment of the operation environment, all the applications loaded as well as related data must be measured and evaluated in terms of trust. In the standards of TCG (Trusted Computing Group), a series of trust measurement about the starting process of the operating system is specified in details, which can be easily implemented in a defined sequence. But the integrity of a running software or application is not specified by TCG, and can be entirely different from the starting process of the system (Li et al., 2010).

The trust evaluation of states mostly relies on the current integrity message and trust measurement collected by the trusted group administrator. There are three ranks of trust defined in this paper, i.e., extremely trusted, critically trusted and untrusted. Suppose $X = \{x_1, x_2, ..., x_n\}$ is a trusted group and x is one entity in X, then $S: x \to [0,1]$ is the trust evaluation function of the entity x. Then,

1 x is untrusted if $0 \le S(x) \le E_0$;

2 x is critically trusted if $E_0 \le S(x) < E_1$;

3 x is extremely trusted if $E_1 \le S(x) < E_2$.

where E_0, E_1, E_2 are predefined thresholds by the administrator and $0 \le E_0 \le E_1 \le E_2 \le 1$.

4.1 Trust evaluation of the starting states

Suppose $BAC = \{\alpha, \beta, \gamma, \eta[1].....\eta[n]\}$ is the basic value of the user's trust measurement, where α is the measured value of BIOS hash calculation, β is the measure value of OS Loader hash calculation, γ is the measure value of OS Kernel hash calculation, and $\eta[1].....\eta[n]$ is the measure values of extended security applications' hash calculation. And supposed $P = \{\alpha', \beta', \gamma', \eta[1]'.....\eta[n]'\}$ is the expected measured value stored by the administrator.

Then, the administrator will compute $R = (\alpha \wedge \alpha') \wedge (\beta \wedge \beta') \wedge (\gamma \wedge \gamma')$. If $R = 0$, the user is totally untrusted and denied of access to the network. Otherwise, define $S(x) = \sum_{i=1}^{n} \eta[i] \wedge \eta[i]'$, and determine x's trust degree following the rules described above: untrusted, critically trusted, extremely trusted.

4.2 Trust evaluation of the runtime states

It is unavailable to collect all runtime integrity messages, so a cycle time T is set by the administrator, which means trust measurement and evaluation of the instant states is performed for every T. And the trust evaluation of one member is always related with all its former behaviours, so we use grey relevance analysis (Kong et al., 2007; Lv and

Ren, 2011) to associate $S: x \to [0,1]$ with its former trust measurements.

Suppose there are n applications $A_1, A_2, ..., A_n$ running in the member x and the trust measurements in the cycle k of all the applications are marked as $P(k) = \{A_1(k), A_2(k), ..., A_n(k)\}$. Then, the collected integrity measurement in all m cycles is

$$P = \begin{pmatrix} P(1) \\ P(2) \\ ... \\ P(m) \end{pmatrix} = \begin{pmatrix} A_1(1) & A_2(1) & ... & A_n(1) \\ A_1(2) & A_2(2) & ... & A_n(2) \\ ... & ... & ... & ... \\ A_1(m) & A_2(m) & ... & A_n(m) \end{pmatrix}$$

where $0 \le A_i(j) \le 1$. The optimal reference data is set as $P(0) = \{1,1,...,1\}$, which is the most trusted as designed. The correlation coefficient between each application A_i in each cycle k and the optimal data can be calculated as

$$\xi_i(k) = \frac{\min_i \min_k |A_0(k) - A_i(k)| + \rho \cdot \max_i \max_k |A_0(k) - A_i(k)|}{|A_0(k) - A_i(k)| + \rho \cdot \max_i \max_k |A_0(k) - A_i(k)|}$$

where ρ is the relative parameter and is usually set as 0.5. The trust evaluation function is then

$$S(x) = \frac{\sum_{i=1}^{n} \sum_{k=1}^{m} \xi_i(k)}{i \cdot m}.$$

Moreover, if each application has a different weigh W_i determined by the network administrator, then,

$$S(x) = \frac{\sum_{i=1}^{n} \sum_{k=1}^{m} (W_i \cdot \xi_i(k))}{i \cdot m}.$$

At last, the network administrator can determine whether member x's current state is trusted by the value $S(x)$ and the thresholds E_0, E_1, E_2.

4.3 Trust evaluation in roaming

For roaming in WMNs, a terminal wants to access its home network through connecting to a foreign network. Since the home network has its predefined thresholds E_0, E_1, E_2 while the foreign network may have a different E_0', E_1', E_2', some merging strategy must be selected to handle the situation by the ISP or the network carriers.

1 Maximum Compatibility Strategy: $\overline{E}_0 = \max(E_0, E_0')$, $\overline{E}_1 = \max(E_1, E_1')$, $\overline{E}_2 = \max(E_2, E_2')$, where $\overline{E}_0, \overline{E}_1, \overline{E}_2$ is the final selected thresholds and $\max(x, y) = \begin{cases} y, & if\ x \ge y \\ x, & if\ x < y \end{cases}$.

2 Minimum Compatibility Strategy: $\overline{E}_0 = \min(E_0, E_0')$, $\overline{E}_1 = \min(E_1, E_1')$, $\overline{E}_2 = \min(E_2, E_2')$, where $\overline{E}_0, \overline{E}_1, \overline{E}_2$ is the final selected thresholds and $\min(x, y) = \begin{cases} y, & if\ x \ge y \\ x, & if\ x < y \end{cases}$.

3 Customisation Strategy: $\overline{E}_0 = f(E_0, E_0', E_1, E_1', E_2, E_2')$, $\overline{E}_1 = g(E_0, E_0', E_1, E_1', E_2, E_2')$, $\overline{E}_2 = h(E_0, E_0', E_1, E_1', E_2, E_2')$, where $\overline{E}_0, \overline{E}_1, \overline{E}_2$ is the final selected thresholds and f, g, h are customised functions by demands.

After the thresholds $\overline{E}_0, \overline{E}_1, \overline{E}_2$ are negotiated between the border routers of the home and the foreign networks, trust evaluation of the starting and the runtime states can be carried out.

1 if it's untrusted, then its request to access the network will be denied;

2 if it's critically trusted, then access will be allowed to an isolated region with limited capability and trust repair is requested. After trusted repair is validated, access can be allowed at the level the extremely trusted degree;

3 if it's extremely trusted, then it can access the network.

5 Roaming protocol for WMNs

Based on the model and the trust evaluation method described above and Elliptic Curve Cryptography (ECC), a trusted roaming protocol is given in this section.

5.1 ECC

In order to achieve better security, the key pair generation and key agreement protocol adopted in this paper are all based on ECC. ECC is chosen because it offers equivalent level of security but with smaller key sizes and faster computation speed compared to some other schemes such as RSA.

All cryptography is built on a suitably chosen elliptic curve E defined over a finite field F_q of characteristic p, and a base point $P \in E(F_q)$. The ECDLP (Elliptic Curve Discrete Logarithm Problem) on $E(F_q)$ is to find an integer m which satisfy $Q = mP$ while P and Q are given. And it is a NP- hard intractability problem.

As described in Law et al. (2003), some domain parameters are defined as follows:

1 a field size q, where q is a prime power (in practice, either $q = p$, or an odd prime, $q = 2^m$);

2 an indication FR (field representation) of the representation used for the elements of F_q;

3 two field elements a and b in F_q which define the equation of the elliptic curve E over F_q (e.g., $y^2 = x^3 + ax + b$ in the case $p > 3$, and $y^2 + xy = x^3 + ax^2 + b$ in the case $p = 2$);

4 a finite point $P = (x_P, y_P)$ of prime order in $E(F_q)$, and $P \neq O$ where O denotes the point at infinity;

5 the order n of the point P, with $nP = O$ and $n > 2^{160}$ as commonly recommended;

6 the cofactor $h = \#E(F_q)/n$, where $\#E(F_q)$ denotes the number of F_q-rational points on E.

Given a valid set domain parameters (q, FR, a, b, P, n, h), an entity A's private key is an integer $\omega_A \in R[1, n-1]$, while its public key is the point $W_A = \omega_A P$. A's public-key certificate, represented as $CERT_A$, contains a string of information that uniquely identifies (such as A's name and address), its public key W_A, the domain parameters if these are not known from context and a certifying authority CA's signature over this information. Any other entity B can use his authentic copy of the CA's public key, which should be broadcasted within the whole network, to verify A's certificate, thereby obtaining an authentic copy of A's public key. In all protocols proposed in this paper, every entity should acquire an authorised certificate from the offline CA before accessing the network.

Three entities A, B and C can complete key agreement as follows:

1 A selects $r_A \in_R [1, n-1]$, computes point $R_A = r_A P$ and sends R_A to B.

2 B selects $r_B \in_R [1, n-1]$, computes point $R_B = r_B P$ and $R_{AB} = r_B R_A = r_A r_B P$, and sends R_A, R_B and R_{AB} to C;

3 C selects $r_C \in_R [1, n-1]$, computes point $R_C = r_c P$, $R_{AC} = r_c R_A = r_A r_C P$, $R_{BC} = r_c R_B = r_B r_C P$ and $R_{ABC} = r_C R_{AB} = r_A r_B r_C P$, and sends R_{AC} and R_{BC} to B;

4 B computes $R_{ABC} = r_B R_{AC} = r_A r_B r_C P$ and sends R_{BC} to A.

5 A computes $R_{ABC} = r_A R_{BC} = r_A r_B r_C P$.

The session key is the point $K_S = R_{ABC}$.

5.2 Terms and notations

Table 1 lists some terms and notations used in this paper. Noted that, $Cert_{AIK}$ is used for proving the identity of the TPM device while $CERT_i$ for proving the identity of the user, and $Cert_{AIK} \neq CERT_i$.

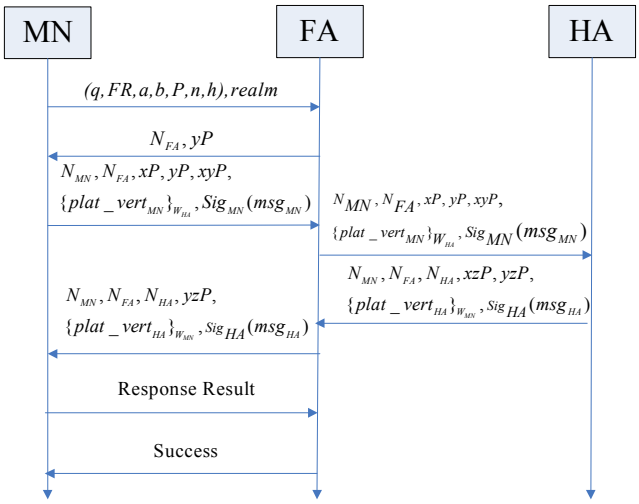
Table 1 Terms and notations

N_i	a random integer generated by i
ID_i	the identity of i
x, y, z	the random integers selected by MN, FA and HA
$plat\_vert_i$	the authentication message to verify i's platform
$Cert_{AIK,i}$, pri_i, pub_i	the AIK (Attestation Identity Keys) certificate of i's TPM with the private and public key pair (pri_i, pub_i) which is issued by the TPM's producer
PCR_i, SML_i	PCR (Platform Configuration RAM) and SML(Store Measure Logs), the integrity verification message of i's TPM
$\{m\}_k$	message m encrypted with key k
$CERT_i, \omega_i, W_i$	the certificate and key pair of i issued by the offline CA
$Sig_i(m)$	the digital signature on message m using i's private key ω_i

5.3 Message flow in trusted roaming

For those who want to roam in a foreign network, no matter what kind of zone networks they belong to, they need to accomplish a three-party authentication with their HA and the FA of the current foreign network. Only a trusted platform operated by a valid user is allowed to access the network.

Figure 3 Message flows in roaming (see online version for colours)



There are seven steps to accomplish an authentication as illustrated in Figure 3:

1 MN sends its home realm's name and corresponding domain parameters (q, FR, a, b, P, n, h) to FA.

2 FA replies N_{FA} and yP to MN, where N_{FA} is a random integer generated by FA and y is a random integer and kept secretly by MN. yP is used to accomplish key agreement, where P is the selected base point of $E(F_q)$;

3 MN constructs $msg_{MN} = N_{MN}, N_{FA}, xP, yP, xyP,$ and its digital signature $Sig_{MN}(msg_{MN})$ and sends them to FA.

a) N_{MN} is a random integer generated by MN;

b) x is a random integer and kept secretly by MN; xP is used to accomplish key agreement, where P is the selected base point of $E(F_q)$;

c) $plat\_vert_{MN} = SML_{MN}, \{ID_{MN}, N_{MN}, N_{FA}, PCR_{MN}\}_{pri_{AIK,MN}}$, $Cert_{AIK,MN}$ where SML_{MN}, PCR_{MN} and $Cert_{AIK,MN}$ are used to ensure MN's platform authentication as well as integrity verification;

d) $Sig_{MN}(msg_{MN}) = \{msg_{MN}\}_{\omega_{MN}}$ is MN's digital signature on the message msg_{MN} with its private key ω_{MN} and is used to authenticate the identity of MN.

4 After receiving the message, FA forwards it to the corresponding HA for further authentication.

5 After receiving the message, HA verifies both MN's identity and platform to ensure that MN is valid under the network's current security policy.

a) HA decrypts $\{plat-vert_{MN}\}_{W_{HA}}$ with its private key ω_{HA} to get $plat-vert_{MN}$. Then HA verifies $Cert_{AIK,MN}$ inside $plat-vert_{MN}$, and decrypt $\{ID_{MN}, N_{MN}, N_{FA}, PCR_{MN}\}_{pri_{AIK,MN}}$ to get ID_{MN} and PCR_{MN}. It can compare PCR_{MN} and SML_{MN} with the reference values of the current network to evaluate MN's platform's trust degree $S(MN)$.

b) HA uses ID_{MN} to get MN's certificate $CERT_{MN}$ which contains MN's public key W_{MN}, and then verifies $Sig_{MN}(msg_{MN})$ to authenticate MN's identity.

c) Only when both verifications are successful, will HA send back its key piece (xzP, yzP) along with its $plat-vert_{HA}$, $Sig_{HA}(msg_{HA})$ to FA, where $plat\_vert_{HA} = SML_{HA}, \{ID_{HA}, N_{MN}, N_{FA}, N_{HA}, PCR_{HA}\}_{pri_{AIK,HA}}, Cert_{AIK,HA}$. And z is a random integer and kept secretly by HA. It can compute the session key $k_S = z(xyP) = xyzP$.

6 FA forwards the receiving message to MN and gets the session key through $k_S = y(xzP) = xyzP$.

7 After receiving the message, MN will do the same verifications as HA did. If successful, MN will get the session key through $k_S = x(yzP) = xyzP$.

6 Security analyses

Formal analysis is currently the most effective way of analysing security protocols among which the strand space model (Thayer et al., 1998) is one of the most effective formal analysis methods. Strand space model is an analysing model of security protocols based on the Dolev-Yao model (1983) built on graph theory and partial ordering and can be used to analyse complicated protocols because of its excellent expansibility. In this section, we formally analyse our proposed protocol with an extended strand space model.

6.1 The enhanced strand model

In the original strand space model, message terms only include atomic terms, encrypted terms and joined terms. Since in our protocol, we have two new operations, i.e., the signature and the DH operations, we will add some new data collections into the model (Shen and Li, 2010; Fang et al., 2008).

Definition 1: *M is a collection of message terms. Term t is an element of M if it is an element of collection T of plaintexts or collection K of key symbols. Complex terms of M are constructed with four operations as follows*:

1 encryption operation, expressed as $\{M\}_K : M \times K \to M$;

2 join operation, expressed as $M_1M_2 : M \times M \to M$;

3 signature operation, expressed as $[M]_K : M \times K \to M$;

4 ECC operation, expressed as $tP : K \times T \to K$.

Definition 2: *A sub-term relation $\angle$ is defined as follows, in which A and N are terms:*

1 $A \angle A$;

2 $k \in K$, if $A \angle N$, then $A \angle \{N\}_k$, especially $k \angle \{N\}_k$ only if $k \angle N$;

3 $N_1 \in M$, if $A \angle N$, then $A \angle NN_1$ and $A \angle N_1N$;

4 $k \in K$, if $A \angle N$, then $A \angle [N]_k$, especially $k \angle [N]_k$ only if $k \angle N$;

5 If $x \in T$ and $x \angle N$, then $xP \angle N$, but not vice versa, especially $x \angle xP$ is disproved, which results from the NP-hard intractability of ECDLP.

Definition 3: *Besides the original eight attack strands, M-strand, F-strand, Tee-strand, C-strand, S-strand, K-strand, E-strand and D-strand, two new attack strands are added:*

1 Sig-strand: $-k, -h, +[h]_k, k \in K, h \in M$.

2 ECC-strand: $-x, -yP, +xyP$.

Definition 4: *K-ideal of collection M is a collection, expressed as $I_K[h] \subseteq M$ that satisfies the following requirements:*

1 $\forall h \in I \forall g \in M$, then $gh \in I$ and $hg \in I$.

2 $\forall h \in I \forall k \in K$, then $\{h\}_k \in I$.

3 $\forall h \in I \forall k \in K$, then $[h]_k \in I$.

6.2 The strand graph

Omitting the information that has nothing to do with security in the protocol, the strand space of our protocol as depicted in Figure 4 can be expressed as a $\sum$ strand Graph. As labelled as p_i in the graph, $plat\_vert_i$ is computed in the TPM's protected functionality and cannot be tampered or faked. And the private and public key (ω_i, W_i) is labelled as (k_i^{-1}, k_i), while the session key is labelled as k_S. Let T_{names} denotes the collection of names and k_P denotes the collection of keys that an attacker has already obtained, then $X \in T_{names}$, public keys $k_X \in K_P$, and the corresponding private keys $k_X^{-1} \in K - K_P$.

1 M1= $N_{FA}(yP)$;

2 M2= $N_{MN}N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}$

$[N_{MN}N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}]_{k_{MN}^{-1}}$;

3 M3= $N_{MN}N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}$

$[N_{MN}N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}]_{k_{MN}^{-1}}$;

4 M4= $N_{MN}N_{FA}N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}}$

$[N_{MN}N_{FA}N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}}]_{k_{HA}^{-1}}$;

5 M5= $N_{MN}N_{FA}N_{HA}(yzP)\{p_{HA}\}_{k_{MN}}$

$[N_{MN}N_{FA}N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}}]_{k_{HA}^{-1}}$;

There are three regular strands in the protocol:

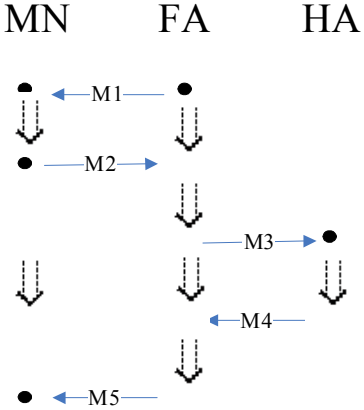
1 $Init[N, N', N'', p, p', k_S]$ is the set of strand $s \in \Sigma$ whose trace is <-M1,+M2,-M5>;

2 $Mid[N, N', N'', p, p', k_S]$ is the set of strand $s \in \Sigma$ whose trace is <+M1,-M2,+M3,-M4,+M5>;

3 $\mathrm{Re}sp[N, N', N'', p, p', k_S]$ is the set of strand $s \in \Sigma$ whose trace is <-M3,+M4>.

Obviously, they are pair-wise disjointed.

Figure 4 Strand graph $\sum$ (see online version for colours)



6.3 Secrecy

Message m is secret in the strand graph G of a protocol if there is no strand n which meets two conditions: $n \in G$ and $un\_term(n) \neq m$.

Theorem 1: *Suppose* C *is a bundle in* Σ *and,* k_S *is uniquely originating. Let* $S = \{k_{MN}^{-1}, k_{HA}^{-1}, k_S\}$ *and* $K^* = K - S$. *Then, for every node* $n \in C$, $term(n) \notin I_{K^*}[k_S]$.

Proof: According to the theory of K-ideal, we just need to prove that no regular node n is an entry point of $I_{K^*}[S]$. We will argue by contradiction and assume that n is a regular node which is an entry point of $I_{K^*}[S]$. Then, one of the keys $k_{MN}^{-1}, k_{HA}^{-1}, k_S$ is a sub-term of $term(n)$. Since there is no regular node contains k_{MN}^{-1}, k_{HA}^{-1} as a sub-term, k_S must be a sub-term of $term(n)$.

$k_S = xyzP$ doesn't appear in any message term, but it can be gained through ECC operations: (1) $x(yzP)$, (2) $y(xzP)$, (3) $z(xyP)$, (4) $xy(zP)$, (5) $xz(yP)$, (6) $yz(xP)$, (7) $x(y(zP))$, (8) $x(z(yP))$, (9) $y(x(zP))$, (10) $y(z(xP))$, (11) $z(x(yP))$ and (12) $z(y(xP))$. The form in which term x appears in all message terms is xP, so $x \angle term(n)$ iff $x \angle xP$. But in our extended strand model, $x \angle xP$ is disproved because of the NP-hard intractability of ECDLP. So $x \angle term(n)$ is disproved and any of y, z, xy, xz, yz cannot be a sub-term of $term(n)$. Hence, the operations listed above cannot carry on in Σ and k_S is not a sub-term of $term(n)$.

Therefore, no regular node n is an entry point of $I_{K^*}[S]$. And for every node $n \in C$, $term(n) \notin I_{K^*}[k_S]$.

6.4 Authentication

A protocol guarantees agreement to a participant B as the responder for certain data items d if every time a participant B completes a run of the protocol as the responder using d, which to B appears to be a run with A, then there is a unique run of the protocol with the principal A as the initiator using d, which to A appears to be a run with B.

Lemma 1. *Suppose* C *is a bundle in* Σ, $X \in T_{names}$ *and* $k_X^{-1} \in K - K_P$, *then no term of the form* $[g]_{k_X^{-1}}$ *can originate on a penetrator node in* C.

Proof: Let $S = \{k_X^{-1}\}$. First, there is obviously no regular node that takes k_X^{-1} as its sub-term. So, k_X^{-1} cannot originate from any regular node and no regular strand is an entry of $I_K[S]$.

Suppose $[g]_{k_X^{-1}}$ originates on a penetrator strand s in Σ. Obviously s cannot be a M-strand, F-strand, Tee-strand, C-strand, S-strand, K-strand, E-strand, D-strand or ECC-strand.

If s is a Sig-strand, then $s =< -k, -h, +[h]_k >$. Since $[g]_{k_X^{-1}} \angle [h]_k$ and $k \neq k_X^{-1}$, we can get that $[g]_{k_X^{-1}} \angle h$. And

since h doesn't originate from s, there must be another strand $s' =< ..., +h, .. >$ that satisfies the condition $s' \to s$, which means that $[g]_{k_X^{-1}}$ doesn't originate from s and it should originate from s', which is a contradiction.

So, no term of the form $[g]_{k_X^{-1}}$ can originate on a penetrator node in C.

Lemma 2: *If* $[H]_{k_X^{-1}}$ *originates on a regular strand* s*:*

1 If $s \in Init[N, N', N'', p, p', k_S]$, then $H = N_A N_B LL'$ in which $N_A, N_B \in T_{names}$ and $L \in K, L' \in M$;

2 If $s \in \mathrm{Re}\,sp[N, N', N'', p, p', k_S]$, then $H = N_A N_B N_c LL'$ in which $N_A, N_B, N_C \in T_{names}$ and $L \in K, L' \in M$;

Proof: s needs to be positive sign.

If s is an Init-strand, then $m =< s, 2 >$ and $term(m) = N_A N_B (K)\{p_A\}_{k_B}\{N_A N_B (K)\{p_A\}_{k_B}\}_{k_A^{-1}}$. At the moment, $H = N_A N_B LL'$.

If s is a Resp-strand, then $m =< s, 2 >$ and $term(m) = N_A N_B N_C (K)\{p_B\}_{k_A}\{N_A N_B N_C (K)\{p_B\}_{k_A}\}_{k_B^{-1}}$. At the moment, $H = N_A N_B N_c LL'$.

Lemma 3: *Suppose* s *is a regular strand in* Σ*:*

1 If $\{N_A N_B LL'\}_{k_X^{-1}}$ originates from s, then $s \in Init[N, N', N'', p, p', k_S]$ and N_{MN}, p_{MN} originate from s.

2 If $\{N_A N_B N_C LL'\}_{k_X^{-1}}$ originates from s, then $s \in \mathrm{Re}\,sp[N, N', N'', p, p', k_S]$ and N_{HA}, p_{HA} originate from s.

Proof: It can be immediately deduced from Lemma 2.

Theorem 2: *(HA's Authentication) Suppose* C *is a bundle in* Σ, N_{HA}, p_{HA} *is uniquely originating in* C *and* $k_X^{-1} \in K - K_P$. *If* $r \in Init[N, N', N'', p, p', k_S]$ *has* $C - height(r) \geq 3$, *then there is a regular strand* $s \in \mathrm{Re}\,sp[N, N', N'', p, p', k_S]$ *and* $C - height(s) \geq 2$.

Proof: the trace of r is:

$$\begin{aligned} r &=< -M1, +M2, -M5 > \\ &=< -N_{FA}(yP), \\ &\quad + N_{MN} N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}} \\ &\quad [N_{MN} N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}]_{k_{MN}^{-1}} \\ &\quad - N_{MN} N_{FA} N_{HA}(yzP)\{p_{HA}\}_{k_{MN}}\{N_{MN} N_{FA} N_{HA} \\ &\quad (xzP)(yzP)\{p_{HA}\}_{k_{MN}}\}_{k_{HA}^{-1}} > \end{aligned}$$

Then $term(< r, 3 >) = N_{MN} N_{FA} N_{HA}(yzP)\{p_{HA}\}_{k_{MN}}[N_{MN} N_{FA} N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}}]_{k_{HA}^{-1}}$ From Lemma 1, $[N_{MN} \; N_{FA} N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}}]_{k_{HA}^{-1}}$ originates from a regular strand in G. From Lemma 3, this strand is $s \in \mathrm{Re}\,sp[N, N', N'', p, p', k_S]$, and $C - height(s) \geq 2$.

Theorem 3: *(MN's Authentication) Suppose* C *is a bundle in* Σ, N_{MN}, p_{MN} *is uniquely originating in* C *and* $k_X^{-1} \in K - K_P$. *If* $r \in \mathrm{Re}\,sp[N, N', N'', p, p', k_S]$ *has* $C - height(r) \geq 1$, *then there is a regular strand* $s \in Init[N, N', N'', p, p', k_S]$ *and* $C - height(s) \geq 2$.

Proof: Proof: the trace of r is:

$$\begin{aligned} r &= \langle -M_3, +M_4 \rangle \\ &=< -N_{MN} N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}} \\ &[N_{MN} N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}]_{k_{MN}^{-1}} \\ &\quad + N_{MN} N_{FA} N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}} \\ &[N_{MN} N_{FA} N_{HA}(xzP)(yzP)\{p_{HA}\}_{k_{MN}}]_{k_{HA}^{-1}} > \end{aligned}$$

Then $term(< r, 1 >) = N_{MN} N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}$ $[N_{MN} \; N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}]_{k_{MN}^{-1}}$ From Lemma 1, $[N_{MN} \; N_{FA}(xP)(yP)(xyP)\{p_{MN}\}_{k_{HA}}]_{k_{MN}^{-1}}$ originates from a regular strand in C. From Lemma 3, this strand is $s \in Init[N, N', N'', p, p', k_S]$, and $C - height(s) \geq 2$.

7 Simulation results

We have performed some simulations using OPNET 14.5 on Windows 7 OS.

7.1 Trust establishment

We performed some simulation using OPNET 14.5 to prove the correctness and the reliability of our scheme in wireless mesh network. The simulation scenario covers an area of 1000m×1000m and all the mobile nodes use a protocol based on IEEE 802.11b. And there are 100 wireless mesh nodes in the network, among which there are a certain amount of untrusted nodes. Some parameters are set as follows: n=10, T=50s, m=10, E0=0.2, E1=0.5, E2=0.8.

Fig. 5 shows the detection rate when there are 15%, 35%, 50%, 75% of the 100 nodes untrusted in the network, whose value is the amount of detected untrusted nodes divided by the amount of all the current untrusted nodes. We can see that, the detection ratio is increasing along with the simulation time, and is going up to 100%. The trust evaluation model is well designed to detect the untrusted nodes effectively in the system.

Fig. 6 shows the detection rate when there are 15%, 35%, 50%, 75% of the 100 nodes untrusted in the network, whose value is the amount of trusted nodes, which are detected to be untrusted nodes in mistake, divided by the amount of all the current nodes. We can see that, the error rate is always less than 10%. The trust evaluation model has a low error rate, due to wireless channel conflicts, network throughout congestion, etc.

Figure 5 Detection ratio of untrusted nodes (see online version for colours)

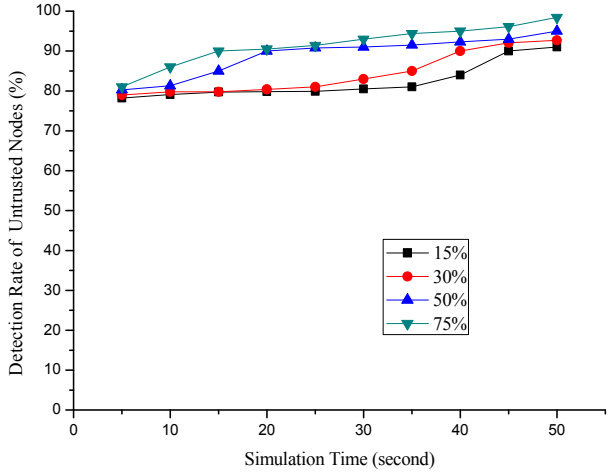
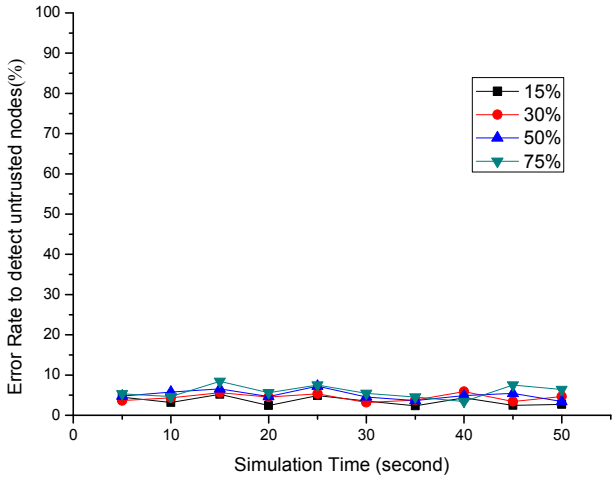


Figure 6 Error rate to detect untrusted nodes (see online version for colours)



7.2 Roaming protocols

Simulations have been performed to compare the protocol we proposed to the EAP-TLS protocol that is widely used in practice and to an ideal EAP-TLS protocol with TPM.

The simulation scenario is set as follows: the network covers an area of 300 km×300 km, network delay is set to be 1 microsecond based on the propagation speed of 300,000km/s by the radio wave and packet loss ratio is set to be at an average of 10% in the network. We carried out 50 simulations in total in which the number of mobile nodes that request roaming service increases from 1 to 50 at an increment of 1. In the beginning of the simulations, all requesting nodes randomly start to request for roaming in 0.5s. The total amount of simulation time is 20s and the number of retries allowed is 3 when authentication fails. In our simulation scenario, one modular multiplication costs about 3ms throughout the experiments.

In the simulations, we compared (1) the success rate of authentication which is defined as the number of MNs successfully getting the roaming service divided by the total number of MNs requesting for roaming service and (2) the average delay of authentication for all the MNs that get the roaming service, and the simulation results are shown in Figures 7 and 8, respectively. We can see from the figures that the success rate of our protocol, which is marked as NEW, is better than both EAP-TLS and EAP-TLS-TPM and average delay of our protocol is also much smaller than that of both EAP-TLS and EAP-TLS-TPM. Compared to EAP-TLS, although the calculation in our protocol takes a little longer time, the communication delay is much smaller, which results in lower average delay.

Figure 7 Success rate (see online version for colours)

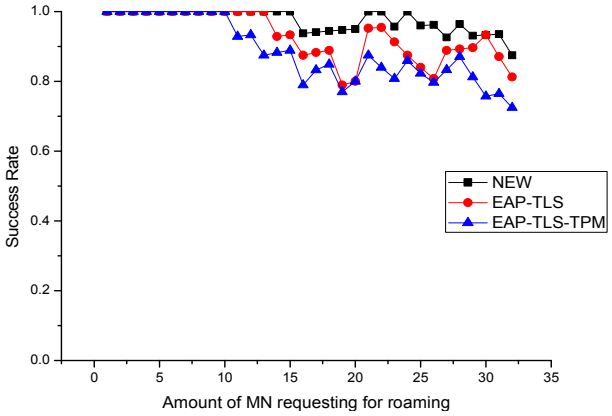
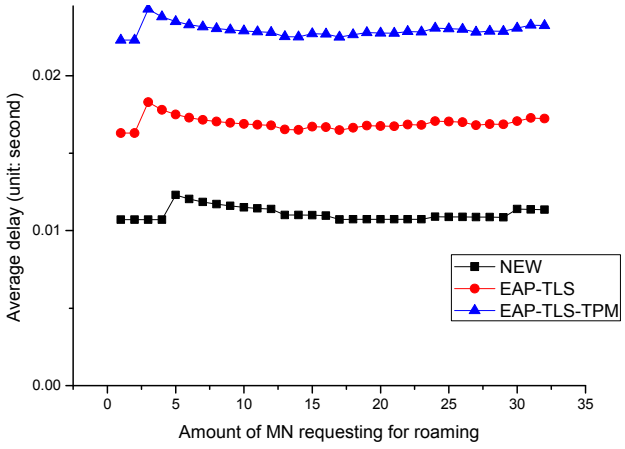


Figure 8 Average delay (see online version for colours)



8 Conclusions

Because of its simple network structure, convenience and expandability, WMN has a broad market prospects, and now it becomes a research focus at home and abroad. However, due to its volatile topology and the characteristics of multi-hop in WMN, the trust and security of roaming in WMN is hard to be guaranteed. A trusted roaming protocol is proposed in this paper based on several technologies, such as hierarchical network model, ECC, trust evaluation, grey relevance analysis and so on. And its security and performance are proved through formal analyses and simulations. In later work, according to its characteristics of WMN, we should increase the success rate and reduce the authentication delay, and provide some valuable results to security research of WMN.

Acknowledgements

The work in this paper has been supported in part by funding from Beijing Natural Science Foundation under grant number 4122009 and in part by funding from National Natural Science Foundation of China under grant number 61272500.

References

Akyildiz, I.F. and Wang, X. (2005) 'A survey on wireless mesh networks', *IEEE Radio Communications*, Vol. 43, No. 9, pp.23–30.

Benyamina, D., Hafid, A. and Gendreau, M. (2012) 'Wireless mesh networks design – a survey', *IEEE Communications Surveys and Tutorials*, Vol. 14, No. 2, pp.299–310.

Cesana, M., Boukerche, A. and Zomaya, A. (2011) 'Security for QoS assured wireless and mobile networks', *Security and Communication Networks*, Vol. 4, No. 3, pp.239–241.

Chen, F. and Gui, X. (2007) 'Research on dynamic trust-level evaluation mechanism based on machine learning', *Journal of Computer Research and Development*, Vol. 44, No. 2, pp.223–229.

Dolev, D. and Yao, A. (1983) 'On the security of public key protocols', *IEEE Transactions on Information Theory*, Vol. 29, No. 2, pp.198–208.

Du, X., Guizani, M., Xiao, Y. and Chen, H. (2009) "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks', *IEEE Transactions on Wireless Communications*, Vol. 8, No. 3, pp.1223–1229.

Fang, Y., Zhang, X. and Zhang, G. (2008) 'Improvement of authentication test based on strand spaces model', *Journal of Computer Applications*, Vol. 28, No. 12, pp.3205–3210.

Finnigin, K.M., Mullins, B.E., Raines, R.A. and Potoczny, H.B. (2007) 'Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.260–271.

Gamer, T., Volker, L. and Zitterbar, M. (2011) 'Differentiated security in wireless mesh networks', *Security and Communication Networks*, Vol. 4, No. 3, pp.257–266.

IEEE (2007) 'Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications', 802.11 Working Group of the IEEE 802 Committee, IEEE P802.11s™/ D1.01, March 2007.

Khan, S., Mast, N. and Loo, K.K. and Silahuddin, A. (2008a) 'Passive security threats and consequences in IEEE 802.11 wireless mesh networks', *International Journal of Digital Content Technology and its Applications (JDCTA)*, Vol. 2, No. 3, pp.4–8.

Khan, S., Mast, N., Loo, K.K. and Silahuddin, A. (2008b) 'Cloned access point detection and prevention mechanism in IEEE 802.11 wireless mesh networks', *International Journal of Information Assurance and Security*, Vol. 3, No. 4, pp.257–262.

Kong, F., Zhang, Z. and Liu, Y. (2007) 'Research on improvement of grey relation analysis method based on ideal points', *3rd International Conference on Wireless Communications, Networking, and Mobile Computing – WiCOM'07*, pp.5712–5715.

Law, L., Menezes, A., Qu, M., Solinas J. and Vanston S. (2003) 'An efficient protocol for authenticated key agreement', *Designs, Codes and Cryptography*, Vol. 28, No. 2, pp.119–134.

Li, D., Yang, Y., Gu, L. and Sun, B. (2010) 'Study on dynamic trust metric of trusted network based on state and behavior associated', *Tongxin Xuebao/Journal on Communications*, Vol. 31, No. 12, pp.12–19.

Lv, F. and Ren, Y. (2011) 'Study on grey relation analysis based on entropy method in evaluation of logistics center location', *Proceedings of the 3rd International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2011*, Vol. 3, pp.474–477.

Ma, Z., Ma, J., Sangjae, M. and Li, X. (2010) 'An efficient authentication protocol for WLAN mesh', *IEICE Transactions on Information and Systems*, Vol. E93-D, No. 3, pp.430–437.

Munoz, A. and Mana A. (2010) 'TPM-based protection for mobile agents', *Security and Communication Networks*, Vol. 4, No. 3, pp.45–60.

Shen, M. and Li, C. (2010) 'Research and analysis on secure DSR routing protocol based on strand space', *International Conference on Electrical and Control Engineering, ICECE 2010*, pp.2917–2920.

Thayer, F., Herzog, J. and Guttman, J. (1998) 'Strand spaces: why is a security protocol correct?', *Proceedings of the 1998 IEEE Symposium on Security and Privacy*, pp.160–171.

Wang, D., Zhou, X. and Zhao, W. (2011) 'Behavior analysis-based dynamic trust measurement model', *Proceedings of Information and Communications Security – 13th International Conference, ICICS 2011*, pp.267–281.

Wang, H., Sheng, B. and Li, Q. (2006) 'Elliptic curve cryptography-based access control', *International Journal of Security and Networks*, Vol. 1, Nos. 3/4, pp.127–137.

Xiao, P., He, J. and Fu Y. (2012) 'A secure mutual authentication protocol for roaming in wireless mesh networks', *Journal of Networks*, Vol. 7, No. 2, pp.267–274.

Yang, C., Cao, C. and Wang, W. (2008) 'New authentication protocol of roaming for wireless mesh network', *Journal of Jilin University (Engineering and Technology Edition)*, Vol. 38, No. 2, pp.423–428.

Yi, P., Xing, H. and Wu, Y. (2009) 'Security in wireless mesh networks: challenges and solutions', *China Communications*, Vol. 6, No. 3, pp.134–140.

Zhang, H., Chen, L. and Zhang, L. (2010) 'Research on trusted network connection', *Chinese Journal of Computers*, Vol. 33, No. 4, pp.706–717.