IADIS International Journal on Computer Science and Information Systems
Vol. 2, No. 1, pp. 1-17
ISSN: 1646-3692

HETEROGENEOUS CERTIFICATE AUTHORITY FOR WIRELESS MOBILE AD HOC NETWORKS (WMANETS)

Iman Almomani *Software Technology Research Laboratory (STRL), De Montfort University, Leicester, LE1 9BH, UK*

Hussein Zedan *Software Technology Research Laboratory (STRL), De Montfort University, Leicester, LE1 9BH, UK*

ABSTRACT

Wireless Mobile Ad hoc NETwork (WMANET) is a group of independent wireless (Mobile/ Semi Mobile) nodes communicating on a peer-to-peer basis with no pre- established infrastructure. The unique characteristics of WMANET make such networks highly vulnerable to security attacks when compared with wired networks or infrastructure-based wireless networks. This paper proposes a novel security algorithm for managing digital certificates when all WMANET nodes are Fully Managed (FM) by other heterogeneous infrastructure-based wireless networks such as WLANs and cellular systems. The new security algorithm, which is called ***FM-WMANET,*** examines the integration of heterogeneous wireless networks to enhance the performance of WMANETs from the security perspectives. FM-WMANET presents a novel integrated key management system that is based on the hierarchal trust models used by the Public Key Infrastructures (PKIs) of extant heterogeneous wireless networks. FM-WMANET is still fully distributed and provides a high level of security, availability, flexibility and efficiency key management services for WMANETs. Graph theory and network simulator NS-2 are used to represent the security system proposed by FM-WMANET, study its performance and demonstrate its effectiveness.

KEYWORDS

WMANET, security, key management, PKI, digital certificates, graph theory, SCC, NS-2.

1. INTRODUCTION

In Wireless Mobile Ad hoc Networks (WMANETs), due to unreliable wireless media, host mobility and lack of infrastructure, providing secure communications is a big challenge in this unique network environment.

The integration of heterogeneous wireless technologies can improve network performance, thereby meeting different security requirements. The research into integrating WMANETs with other wireless networks such as cellular networks can be found in (Hsieh and Sivakmar 2001, Lin and Hsu 2000 and Wu et al 1994). These focus on how WMANETs can enhance cellular services. This paper utilize from the integration of heterogeneous wireless networks to improve the performance of WMANETs from the security perspectives.

Usually cryptography techniques are used for secure communications in wired and wireless networks. Cryptography is an important and powerful tool for security services, namely authentication, confidentiality, integrity, and non-repudiation. It converts readable data (plaintext) into meaningless data (ciphertext). Cryptography has two dominant flavors, namely symmetric-key (secret-key) and asymmetric key (public-key) approach. There is a variety of symmetric or asymmetric algorithms available, such as DES, AES, IDEA, RSA, and EIGamal (Schneier 1996, Stallings 2003).Threshold cryptography (Shamir 1979) is a scheme quite different from the above two approaches. In Shamir's (k, n) secret sharing scheme, a secret is split into n pieces according to a random polynomial. The secret can be recovered by combining k pieces based on Lagrange interpolation.

In fact, any cryptographic means is ineffective if the key management is weak. Key management is a central aspect for security in WMANETs which requires an effective management of digital certificates.

In cryptography, a digital key certificate is a certificate which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a *typical public key infrastructure (PKI) scheme*, the signature will be of a Certificate Authority (CA). X.509 is a widely used standard for defining digital certificates following the above scheme. It is published as ITU recommendation ITU-T X.509 (ITU-T X.509 2005).

In a *web of trust scheme*, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. Examples of implementations of this approach are GPG (The GNU Privacy Guard), and PGP (Pretty Good Privacy) (Zimmermann1995, Garfinkel 1995).

Current approaches for managing the digital certificates in ad hoc networks are utilizing one of the above two approaches, PKI or the web of trust. While both approaches have different advantages and limitations, neither approach is effective in all scenarios, as we are going to show in the next section.

The security algorithm proposed in this paper will be compared to those that adopt the PKI approach. In previous work, to adapt PKI to ad hoc networks, threshold cryptography is used to provide a virtual CA comprised of multiple mobile nodes that collectively provide certification services.

In this paper we propose a novel, efficient, security algorithm (FM-WMANET) for managing the digital certificates in WMANET. We will take the assumption that WMANET

exists in heterogeneous wireless environment. The novel algorithm is still fully distributed, provides a high level of security, availability, flexibility and efficiency key management services for WMANETs.

The following sections present the network model constituting the basis of FM-WMANET. The key management system representation is illustrated, the FM-WMANET certificates management framework is defined and the means of coping with misbehaving nodes in this algorithm is explained. Finally, FM-WMANET will be evaluated and the corresponding results discussed and analysed.

2. RELATED WORK

Solutions to the problem of pubic key management in WMANETs have already been proposed; they are utilizing one of the above two approaches, PKI or the web of trust. To adapt PKI to ad hoc networks, threshold cryptography is used to provide a *virtual* Certificate Authority (CA) comprised of multiple mobile nodes that collectively provide certification services.These solutions are briefly summarized in this section.

(Zhou and Haas1999) propose a distributed public-key management service for ad hoc networks. The service, as a whole, has a public/private key pair K/k that is used to verify/sign public-key certificates of the network nodes. It is assumed that all nodes in the system know the public-key K and trust any certificates signed using the corresponding private key k. The private key k is divided into n shares using an (n, t+1) threshold cryptography scheme, and the shares are assigned to n arbitrarily chosen nodes, called servers. For the service to sign a certificate, each server generates a partial signature for the certificate using its private key share and submits the partial signature to a combiner that computes the signature from the partial signatures. The application of threshold cryptography ensures that the system can tolerate a certain number $t < n$ of compromised servers in the sense that at least t+1 partial signatures are needed to compute a correct signature. This proposal, however, assumes that there is an authority that initially empowers the servers and that some of the nodes must behave as servers. It also doesn't describe how a node can contact t servers securely and efficiently in case that the servers are scattered in the whole area. The distribution of refreshed secret shares in an efficient and secure way is not addressed too.

In more recent proposal, that is first described by (Luo and Lu 2000) and later analyzed by (Kong and Zerfos 2001). It provides a more fair distribution of the burden by allowing any node to carry a share of the private key of the service. However, just like in Zhou and Haas proposal (Zhou and Haas 1999), the first t+1 nodes must be initialized by a trusted authority. In addition to this drawback, there are other two problems with this proposal. First, the number t must be a trade off between availability and robustness; but, it is not clear how the value of t can be changed when the overall number of nodes significantly increases (or decreases). Second, the system seems to be vulnerable to the Sybil attack (Douceur 2002): An attacker can take as many identities as necessary to collect enough shares and reconstruct the system's private key. There are many other approaches also depend on building virtual certificate authority using threshold cryptography such as those presented in (Luo et al. 2002, Khalili et al. 2003, Narasimha et al. 2003, Yi and Kravets 2003, Xu and Liviu 2004).

The web of trust model fits naturally with ad hoc networks with its decentralized distributed environment. There is no professional Certificate Authority (CA). The nodes

themselves are responsible for issuing and managing the digital certificates for each other. The authors (Hubaux et al. 2001, Capkun et al. 2003, et al. Capkun 2003) involve this model in their research. They propose a fully self organized public key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication without any centralized services. However, this approach requires a warm up period to populate the certificate graph, which completely depends on the behavior and mobility of the nodes. In addition to that, there is no guarantee that the resulting certification graph will dense enough to authenticate all the public keys in the network. Finally, the validity of a certificate chain depends only on the trustworthiness of the nodes in this chain, which may not suitable for applications where high degrees of accountability and security are required.

FM-WMANET is compared with the previous work that adapted the PKI approach. FM-WMANET deals with real CAs with the highest level of security and availability, rather than the virtual CAs applied in previous researches. Use of threshold cryptography entails a higher maintenance overhead than is the case with real CAs. In addition, all the nodes will be treated equally; there are no servers or combiner nodes.

3. NETWORK MODEL

The network model of the FM-WMANET algorithm is based on our WMANET architecture (Almomani et al. 2005, Almomani et al. 2006). In this algorithm all the nodes comprising the ad hoc networks are involved in other infrastructure-based wireless networks such as WLAN and cellular systems. Therefore, each of the ad hoc nodes will belong to some PKI, as shown in Figure 1.

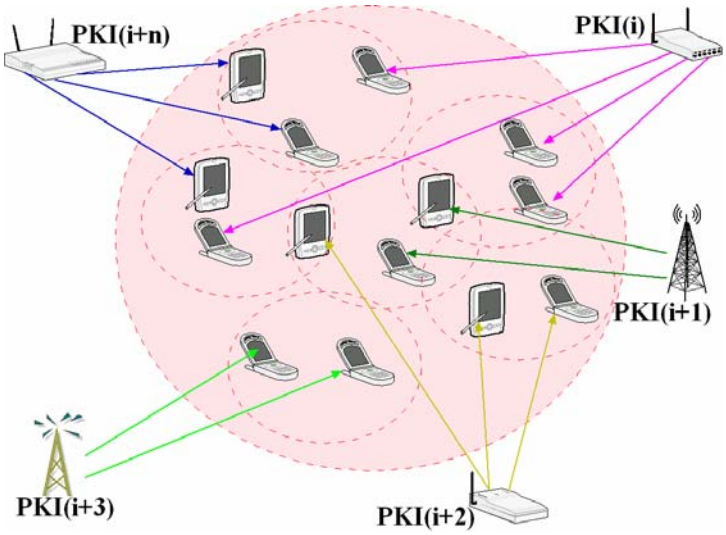

Figure 1. Network model of FM-WMANET

Each PKI has a CA which is fully trusted by all nodes belong to this PKI. It is relatively uncommon to have one node that belongs to more than one PKI, because this protocol is used in civilian environments where the number of PKIs within a given area is limited. This will include the PKIs of the known mobile operators and wireless LANs in that area.

4. SYSTEM REPRESENTATION

The key management system of the FM-WMANET is represented as a directed graph G (V, E) called the *Certification Graph (CG)*. The vertices (V) stand for the public keys of WMANET nodes and the edges (E) stand for their digital certificates. **There is a directed edge from vertex Pk_x to vertex Pk_y if *x*, key holder of Pk_x, believes that digital certificate binding Pk_y to *y* is correct.**

This belief is based on the hierarchal trust model used in this algorithm. Each extant PKI has a CA which is full trusted by all nodes belong to this PKI. Therefore, if there are two nodes *x* and *y* belonging to the same PKI, there will be a directed edge from the public key of *x* to the public key of *y* and vice versa, as shown in Figure 2.

Figure 2. Graph representation of the FM-WMANET key management system

5. FM-WMANET CERTIFICATE MANAGEMET FRAMEWORK

This section describes the certificate management system of FM-WMANET which is briefly introduced in (Almomani and Zedan 2007). It shows how public/private keys and digital certificates are created, explains how the CG is generated and presents the pseudo-code of the FM-WMANET algorithm. It also illustrates the process of certificate revocation.

5.1 Creation of Public/Private Keys and Digital Certificates

The public keys and the corresponding private keys of WMANET nodes are created by the CAs of their PKIs. The public-key certificates of WMANET nodes are also issued by these CAs. Each WMANET node will hold its digital certificate in its Local Database (LDB). The main structure of FM-WMANET digital certificates is shown in Figure 3. It contains the identifier of the WMANET node, its public key, the name of the CA issuing this certificate, the certificate issue and expiry dates and the public key of the CA. Finally, the contents of the certificate will be attached to the digital signature of the CA.

Node Identifier (ID)- Name
Node Public Key (pk)
Certificate Authority (CA) Identifier- Name
Certificate Issue Date/Time
Certificate Expire Date/Time
CA public key (pk(CA))
CA Digital Signature

Figure 3. The structure of the FM-WMANET digital certificates.

5.2 Creation of Digital Certification Graph

Suppose that WMANET consists of the following nodes: A, B, C, D, E, F, G, H, I, and that it is covered by three different PKIs (PKI1, PKI2, and PKI3). The distribution of WMANET nodes to these PKIs is shown in Figure 4.

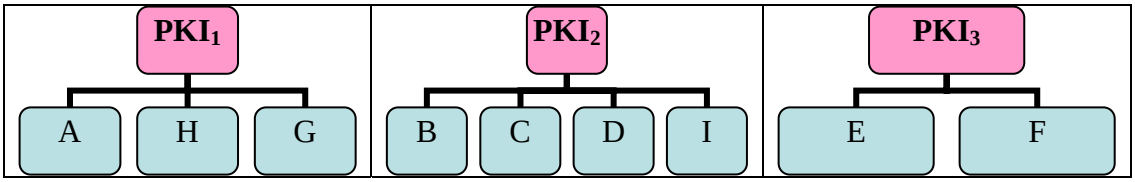

Figure 4. The set of PKIs exist the WMANET

A node can verify the certificate of any other node belonging to the same PKI, because all their certificates are signed by the same CA, which is completely trusted by all of them. The complete certification graph in this case is shown in Figure 5. The total number of edges can be calculated using the formula

$$\sum_{PKI\ i=1}^{PKI\ i=n} \binom{m_i}{2}$$

where mi= the number of nodes belong to PKI_i

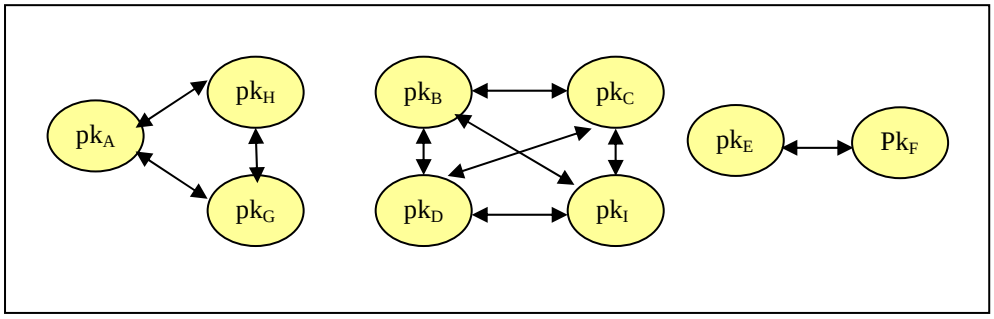

Figure 5. The CG of FM-WMANET.

5.3 Digital Certificates Exchange

The Certificate Exchange is a very important and low-cost mechanism that allows WMANET nodes to distribute the certificates they hold. Each node periodically sends its physical neighbour (in one hop) the digital certificates and the corresponding CA's public key stored in its LDB. When the neighbours receive these certificates, they compare them with their LDBs and add whatever new certificates they do not hold, as well as the public keys of their issuers or they add the renewal of an expired, extant certificate. The certificates exchange process is repeated at a specified time interval called the Exchange Time Interval (ETI). After a certain time, all nodes will have almost the whole certification graph shown in Figure 5.

5.4 FM-WMANET Pseudo-Code

As mentioned in Section 5.1, all digital certificates of WMANET nodes are issued by professional CAs. Each CA first generates the public/private key pairs for nodes belonging to it. Then the CA issues a digital certificate binding each public key with its owner and signs it by its private key. The CA provides each node with its digital certificate and CA public key. Each node in the WMANET has a Local DataBase (LDB). In the initial phase of the system, each node holds in its LDB the digital certificate issued by the CA belong to its PKI and the public key of this CA.

When node *x* wants to communicate securely with node *y*, it searches for the *y* certificate in its LDB. When that is found, the node checks the CA of *y*. If both nodes have the same CA, *x* uses the public key of its CA to validate the digital certificate of *y*. *X* then uses the public key provided in this certificate to send data to *y* in a secure manner. But if they do not have the same CA, *x* will validate the certificate of *y* using the CA's public key provided with this certificate and, if the validation is successful, will crosscheck the public key of the CA. It does this by searching' its LDB for other certificates signed by the same CA and compare the public key of this CA with the public key of *y*'s CA.

If node *x* does not find the digital certificate of *y* in its LDB, then *x* contacts *y* and requests its digital certificate. Additionally, both nodes merge their LDBs as another way to exchange the digital certificates. The certificate of *y* now is added to the LDB of *x*. Therefore, *x* can repeat the steps mentioned above in validating this digital certificate.

It is important during the validation of a certificate to make sure it is not expired. Therefore, a request for a certificate could be made when it is expired and needs to be renewed, as well as when it is not found in the LDB.

In the implementation of the security protocol FM-WMANET, WMANET nodes try three times to authenticate a key. The time between each retry and the next is called the Authentication Time Interval (ATI). After the three retires, if the key still can not be validated, authentication of this key has failed. The FM-WMANETs pseudo-code is shown in Figure 6.

5.5 Digital Certificates Revocation

Certificate Revocation is one of the basic services that should be provided by any digital certificate management system. In this algorithm there are two types of certificate revocation:

- **Explicit revocation:** when the CA belong to PKIi revokes a certificate that it has issued for one of its nodes, and sends the corresponding revocation to the other nodes

belonging to the same infrastructure. If this is not possible for any reason such as the nature of the wireless network of this PKI_i, the renewal of this certificate could be ended, resulting in an implicit revocation.

- **Implicit revocation:** Each certificate is revoked after its expiration time. In general each certificate contains its issuing and validity times as determined by the issuer. Each PKI_i should therefore update the certificates of its nodes before the expiration time.

In both types of revocation, any information provided by the CA to its nodes about any certificate should be distributed though the exchange process. In this way the nodes belong to other CAs will be provided with this new information.

Consequently, FM-WMANET does not concern itself mainly with the certificate revocation process, indeed, this is considered as one of its advantages. Both types of revocation are derived from the extant PKIs. FM-WMANET is only responsible for transferring these revocations to all WMANET nodes.

All of a PKI's nodes are informed when any of them carries out an explicit revocation, and their LDBs are subsequently modified. This revocation will be transferred to the other PKIs' nodes, both by certificate exchange and the LDBs merging process.

The CAs of the PKIs are responsible for updating those certificates that have been implicitly revoked. Once the node has got its new certificate it will update its LDB and then communicate the new certificate to its neighbours through the certificate exchange process. If one of the nodes does not receive the new certificate through the exchange and merging processes and needs to validate the key, the new certificate will be requested from the node itself.

6. COPING WITH MISBEHAVING USERS

In the FM-WMANET algorithm, it is more difficult task for a malicious node to make other nodes accept a false certificate. This is because all the certificates in this algorithm are issued by a professional CAs. The dishonest node can try to do the following:

1. Issue a certificate for itself or for any other node. It then signs this certificate with its private key, claims that this certificate is signed by a professional CA and uses its public key as the CA public key (this is because FM-WMANET requests that each node must hold the digital certificate and the corresponding public key of the CA).
2. Issue a certificate for itself or for any other node. It then signs this certificate with its private key and claims that this signature belongs to a professional CA; this time, however, it uses the real public key of the CA to be attached to the certificate. This node can get the real public key through other certificates properly signed by this CA.

FM-WMANET:

Pk(x): public key of node x

Prk(x): private key of node x

N: number of PKI covered the WMANET

PKIi: Public Key Infrastructure i, i=1… n

CA(x): Certificate Authority issued digital certificate for x

DC(x): Digital Certificate of node x

LDB(x): Local Database of x

ETI: Exchange Time Interval

ATI: Authentication Time Interval

CA (PKIi): Certificate Authority of PKI_i

// Generation of the private/public keys of the WMANET nodes

FOR i= 1 … n

Generate pk(x)/prk(x), $\forall$ x $\in$ PKI_i

//Issuing the Digital Certificates

FOR i=1… n

Issue DC(x) $\forall$ x $\in$ PKI_i

Sign DC(x) with prk ($CA(PKI_i)$)

//Exchanging the Digital Certificates

Repeat every **ETI**

$\forall$ x $\in$ WMANET

Exchange (DC(x)) AND pk (CA(x))) TO neighbour(x),

Store (DC (neighbour(x)) AND pk (CA (neighbour(x))) IN LDB(x)

// Key authentication

IF x want to authenticate pk(y) THEN

Check (LDB(x))

IF (DC(y) = available) THEN

IF (CA(x) = CA(y)) THEN

Validate DC(y) using pk (CA(x))

ELSE

Validate DC(y) using pk (CA(y))

Compare pk (CA(y)) AND pk (CA (z)), where CA(y) = CA (z), z $\in$ LDB(x), z $\neq$ y

ELSE

Request (DC(y))

Request (LDB (y))

Merge LDB(x) AND LDB(y)

Repeat key authentication process after **ATI**

Figure 6. FM-WMANET algorithm pseudo code

3. Issue a certificate for itself or for any other node. It then signs this certificate with its private key and claims that this certificate is signed by a non-existent CA; in this case it uses the corresponding public key attached to the certificate as if it is the public key of this CA.

All these types of malicious behaviour can be detected and prevented by the FM-WMANET algorithm. Referring to FM-WMANET's pseudo-code, which is defined in Section 5.4, the authentication within a different CA of the key of a node should pass two conditions:

- the signature should be validated with pk(CA)
- the pk(CA) should be compared with other pk(CA)s attached to the certificate issued by the same CA

In the first case, when any node *x* attempts to validate this certificate, the validation process will end successfully because the certificate is signed by the private key which corresponds to the public key attached to the certificate. But there is another condition. *X* will compare this attached public key with other public keys attached to certificates issued by the same CA. In this case there will be a mismatch, the origin of which will be clear. This node will then develop a bad reputation.

In the second case, the validation process will fail. This is because the certificate is signed by the private key of the node and attached to the public key that is not the one corresponding to the node, but is rather the authentic public key of the CA. In this case there is no need to check the other condition.

In the third case, the signature's validation will be successfully completed because the private key which signs this certificate corresponds to the public key attached to it, as if it is the public key of the CA. However, the comparison of the pk(CA) with others for the same CA attached to other certificates could have one of two results.

- **If the malicious node is working individually**, this certificate will be the only false certificate holding the name of the non-existent CA. The comparing condition will therefore fail, since there no other certificates issued with the same fake CA available in the LDB, even after waiting some time for the possibility of receiving another certificate with the same CA.
- **If the malicious node is working in groups**, in a similar manner to Sybil attacks, there will be a set of nodes with different identities that sign certificates for themselves or for each other. They do this after agreeing on one private/public key pair and one CA name. In this case it is a possible to find another certificate in the LDB signed by this false CA. This can be resolved based on the proposed network model assumption. The network model of FM-WMANET assumes the WMANET applications in the civilian environments.

  The area that could be covered by WMANET is limited, and consequently so is the number of PKIs. This includes the number of known mobile operators in this area (cellular systems), as well as the available WLANs that belong to some governmental or commercial places. Therefore, these CAs should be familiar and pre-determined; consequently, any forged CA should be easily detected, especially if there is cooperation between these networks. This cooperation could benefit not only WMANETs but also these infrastructure-based wireless networks.

7. FM-WMANET EVALUATION

This section explains graph-theory-based study and NS-2-based study of the FM-WMANET algorithm. The experimental results of these two studies will also be presented and analysed.

7.1 Graph-Theory Based Evaluation

Graph theory algorithms have been applied to study the CGs generated by the FM-WMANET algorithm. C++-based software has been developed to simulate FM-WMANET and test its performance based on two evaluation metrics.

- **Certification graph connectivity:** In graph theory, a directed graph is called "strongly connected" if for every pair of vertices u and v there is a path from u to v and a path from v to u. The main term related to graph connectivity which was used in the experimental analysis for the present study is *Strongly Connected Components (SCC)*. The SCC of a directed graph is its maximal strongly connected subgraph. By studying the connectivity of the CG, the performance of the FM-WMANET can be measured. This means, ***the more connected the certification graph, the more successful the key authentication.***
- **Security level:** This evaluation metric is related to the number of PKIs extant in WMANET. When most of the nodes belong to the same PKI, the authentication process will be highly secure. This does not mean that the greater the number of PKIs the less the percentage of keys which are authenticated, but authentication will be less secure with a greater number of PKIs because nodes from different PKIs will be needed to authenticate keys. Although the FM-WMANET algorithm has dealt with this, it still does not reach the security level of authenticating keys belong to the same PKI, unless there is pre-agreement between these PKIs.

The effect of the number of PKIs in WMANET on the connectivity of the CG has been studied. The simulation results shown in Figure 7 indicate that the fewer the number of PKIs the more connected the CGs and vice versa. In the former case key authentication is performed very securely because most (or all) of the nodes have certificates issued by the same trusted third party. The fact that a CG is less connected does not imply that the key authentication process will fail, but it will be less secure because it will have digital certificates from different professional issuers. As shown in Figure 7, increasing the number of PKIs will reduce the SCC till it reaches 1, which is the minimum it could reach. This will happen when each node in WMANET belongs to a different PKI. On the other hand, decreasing the number of PKIs to one PKI will give strongly connected graph with the maximum value of SCC, which will be the number of nodes in this case.

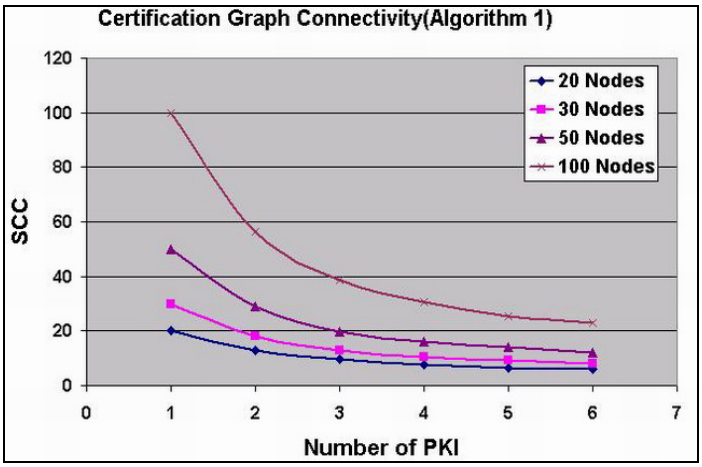

Figure 7. Certification graph connectivity of FM-WMANET

It can be also observed from these results that the behaviour of FM-WMANET is the same irrespective of the number of nodes being applied. Thus, this ensures that FM-WMANET algorithm satisfies the scalability factor.

7.2 NS-2 Based Evaluation

The latest version of NS-2 (NS-2 home page, Fall and Varadhan 2003 and Altman and Jimenez 2003), version 2.30, was used to simulate the security protocol FM-WMANET. NS-2 simulator is installed in the Linux-based operating system Ubuntu 6.06. In order to reduce the effect of randomisation used in the simulation, each experiment was executed 30 times and the average calculated. In the NS-2 based study, the performance of FM-WMANET was evaluated using the following metrics: **Success Ratio** measures the ratio of the number of successful key authentication requests to the total number of key authentication requests that should take place during the simulation time. **Average Delay** measures the average latency to successfully authenticate a key. **Overhead** measures the total number of packets transmitted as part of the of the FM-WMANET communication protocol to provide the key authentication service. Finally, **Average Number of Retries** measures the average number of attempts made before a node successfully authenticates a key. Each metric mentioned above has been simulated in three different scenarios: *Mobility scenario* with different pause time values (0, 10, 30, 50, 70, 100), *Speed scenario* with different node speeds (1, 5, 10, 15, 20, 25, 30) and *Network sizes scenario* with different number of nodes (10, 30, 50, 70).

The Figures (8-9) will show the success ratio versus the three different scenarios of speed, mobility and network size. It is assumed that each node will make at least one authentication request. Therefore, the total number of authentication requests made during the simulation time is equal to the number of nodes.

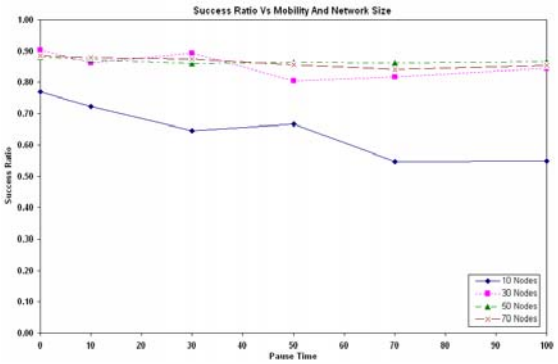

Figure 8. Success ratio versus mobility and network size

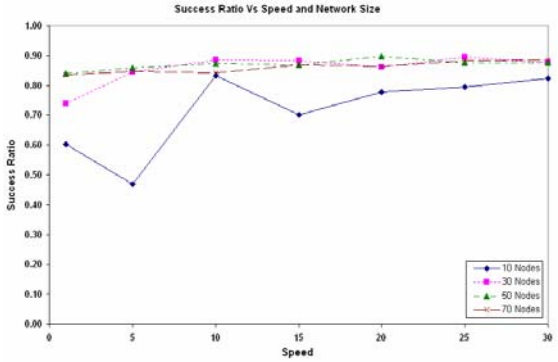

Figure 9. Success ratio versus speed and network size

Figure 8 shows the success ratio against mobility and network size. Mobility is most often a big issue in developing ad hoc protocols. As can be seen, FM-WMANET is not much affected by mobility. In general, the success ratio increases with high mobility situations (less pause time) and large network sizes. Moreover, the effect of mobility is more noticeable with a small number of nodes, especially if that number falls below 30. This is due to the number of neighbour nodes. For example, when the network size is 10, the number of neighbours is around 1.96, but when the network size is 30 the number of neighbours is more than 6. Therefore, the effect of mobility increases with a lesser number of nodes, because less mobility reduces the effect of fewer neighbourhoods.

Figure 9 shows the success ratio against speed and network size. The FM-WMANET is not strongly affected by speed, but in general, as speed increases so does the success ratio. The influence of speed is more noticeable with small network sizes in a manner similar to that of mobility. FM-WMANET provides a better success ratio in large network sizes.

The Figures (10, 11) show the average delay versus mobility, speed and network size scenarios. Regarding mobility, the average delay reduces by decreasing the pause time as shown in Figure 10.

In addition to that, large network size will lead to an increase in the average delay. Increasing the network size will increase the communication load which means: more waiting in the links' queues, more dropping packet, more number of retries and consequently causing more delay. The queue size used in the experiments was 50 packets. The impact of the network size on the delay appears when the network size is 30 nodes or more.

As speed increases, the average delay decreases as shown in Figure 11. In case of network size less than 30 nodes, the average delay was lower comparing with networks size greater than 30 nodes.

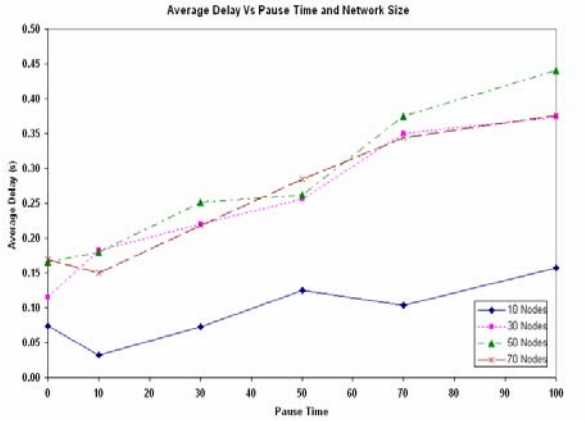

Figure 10. Avg delay against mobility and network size

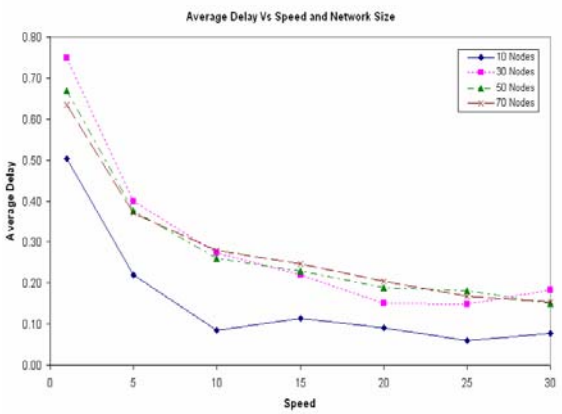

Figure 11. Average delay against speed and network size

Figures (12, 13) demonstrate the overhead of FM-WMANET in terms of the number of packets generated by this security protocol. The overhead has been studied against the network mobility, speed and size. As mobility decreases the overhead slightly increases especially when network size is greater than 10 nodes as depicted in Figure 12. It is also obvious from this figure that overhead increases by increasing the network size.

As the node speed increases, it is observed that the overhead almost remains unchanged for FM-WMAMET (Figure 13); the overhead slightly decreases when the speed increases. Figure 13 assures the increase of overhead by increasing network size.

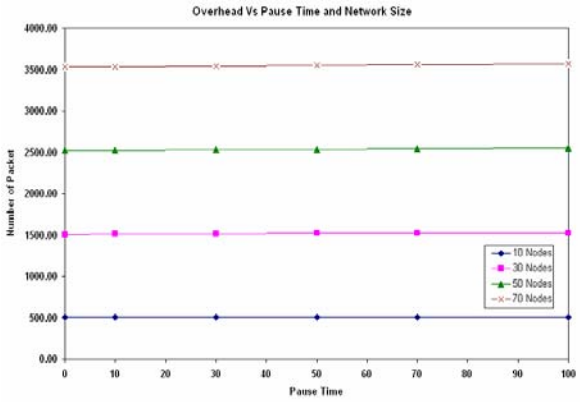

Figure 12. Overhead versus mobility and network size

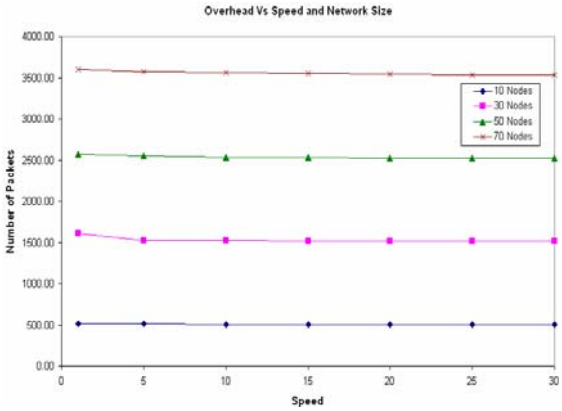

Figure 13. Overhead versus speed and network size

In general, the average number of retries increases as the mobility decreases and as the speed also decreases as can be seen in Figure 14 and Figure 15. It can be also observed in these two figures that the average number of retries is not enormously influenced by the network size.

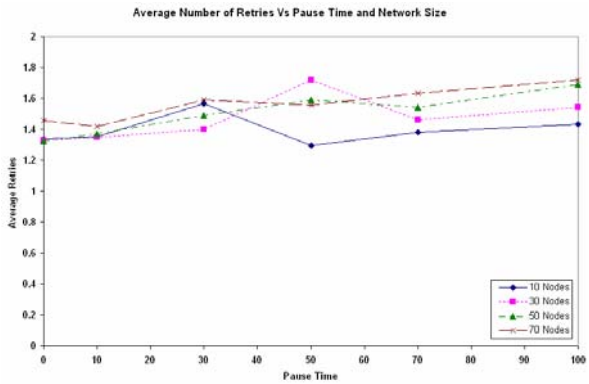

Figure 14. Average number of retries against mobility and network size

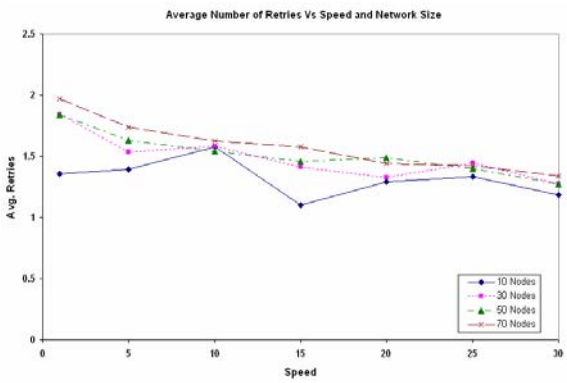

Figure 15. Average number of retries against speed and network size

FM-WMANET was simulated in different scenarios with wide range of parameter values. The corresponding results give clear idea about the performance of FM-WMANET in real network environment.

In real applications of the FM-WMANETs, parameter values could be selected based on the business requirements of the applications themselves. Consequently, high priority could be given to some evaluation metrics more than others, which will certainly affect the choice of the parameter values.

8. CONCLUSION

A novel security protocol for managing the digital certificates in a Fully Managed WMANET called FM-WMANET is proposed. This protocol assumes that all WMANET nodes are part of other infrastructure-based wireless networks. Using small portion of information from these wireless networks has provided a big improvement in managing the digital certificates in WMANET. The trust model used by the FM-WMANET is a heterogeneous hierarchal trust model.

FM-WMANET is evaluated using graph theory and NS-2 simulator. The results of the evaluation confirm that FM-WMANET is a fully distributed security protocol that provides high level of security, availability, flexibility and efficiency key management services for WMANETs.

It is obvious that FM-WMANET is a ***fully distributed*** security protocol. It does not depend on any centralisation in issuing, managing and validating the digital certificates of WMANET nodes.

Key management system provided by the FM-WMANET is ***highly secure***. It supplies WMANET with digital certificates issued by real, professional CAs rather than virtual CAs applied in previous researches. These researches have serious shortcomings regarding the level of security given, assumptions taken and the total computation and communication costs as discussed in Section 2. In addition to that, FM-WMANET proved its ability to cope with different types of security attacks.

FM-WMANET improves the ***availability*** of the key management service in WMANET. This is due to the support taken from the extant infrastructure-based wireless networks. There is no full dependency on the ad hoc nodes themselves to provide all the services of the key management system, especially when there is no guarantee of having honest, collaborating ad hoc nodes all the time. Availability has been shown in the results in terms of delay and average number of retires. The maximum delay recorded from all experiments in all scenarios was less than 0.75 second. Moreover, the average number of retires didn't reach 2 retries. Hence, FM-WMANET supplies a high available key management service of WMANET.

Interesting observations from the experiments that intended to test the impact of the network size on the performance of FM-WMANET is that this security protocol is ***scalable***. In terms of success ratio the FM-WMANET provides high success ratio with large networks sizes. Both delay and average number of retries are not very affected by the network size. There was a slight increase in them while increasing the network size. An increase in the network size logically leads to an increase in the number of transferred packets which therefore, increases the network overhead.

Applying FM-WMANET successfully could be achieved in different scenarios and applications. It offers ***flexibility*** in different terms. There are no constraints or conditions to apply the FM-WMANET except the network model that assumes that WMANET is operating in heterogeneous wireless networks. As shown by the experimental results, FM-WMANET performed very well with different numbers of: PKIs, network size, pause times and speeds. It is also explained that FM-WMANET could be applied using one PKI in case of integrating with cellular networks. It can also provides the same level of efficiency with more than PKIs in case of having a collaborative wireless networks.

Based on the evaluation metrics including success ratio, delay, number of retries and overhead that used to test the performance of FM-WMANET, the results of both the graph theory and NS-2 studies show an ***efficient*** key management service provided by FM-WMANET.

REFERENCES

Almomani, I. et al, 2006. “Architectural framework for wireless mobile ad hoc networks “, Computer Communications**,** Vol. 30, No. 1, pp 178–191.

Almomani, I. et al, 2005. “Architectural Framework for Wireless Mobile Ad hoc Networks (WMANETs)”, The 6th IEE INTERNATIONAL CONFERENCE ON 3G & BEYOND (3G 2005), The IEE, Savoy Place, London, UK.

Almomani, I. and Zedan, H., 2007. “Secure Distributed Key Management for Wireless Mobile Ad hoc Networks (WMANETs)”, IADIS International Conference Applied Computing 2007, Salamanca, Spain.

Altman, E. and Jimenez, T., 2003. “NS2 for beginners”, lectures notes 2003-2004, University of de Los Andes, France.

Capkun, S.; Buttyan, L. and Hubaux, J-P. 2003. “Self-organized public-key management for mobile ad hoc networks”, Mobile Computing, IEEE Transactions, p. 52-64.

Capkun, S.; Hubaux, J-P. and Buttyan, L. 2003. “Mobility helps security in ad hoc networks,” in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003).

Douceur, J. R. 2002. “The Sybil Attack”, Electronic Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02).

Fall, K. and Varadhan, K., 2003. “The ns Manual (formerly ns Notes and Documentation)”, The VINT Project.

Garfinkel, S. 1995.“PGP : pretty good privacy”, Minor corr. March 1995 ed., Beijing: O'Reilly & Associates. xxxiii, 393 p.

Hsieh, H.Y. and Sivakmar, R., 2001. "Performance comparison of cellular and multi-hop wireless networks: a quantitative study", Proceedings of ACM SIGMETRICS 2001, pp. 113–122

Hubaux, J.; Buttyan, L. and Capkun, S. 2001. “The Quest for Security in Mobile Ad Hoc Networks”, in Mobile ad hoc networking & computing, Long Beach, CA: Ieee.

ITU-T Recommendation X.509 , “Public-key and attribute certificate frameworks ”, August 2005.

Khalili, A., J. Katz, and W.A. Arbaugh. 2003. “Toward secure key distribution in truly ad-hoc networks”, in Applications and the Internet Workshops,. Proceedings. 2003 Symposium.

Kong, J. and Zerfos, P. 2001. “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks”, Proc. Ninth Int’1 Conference, Network protocols(ICNP).

Lin, Y.D. and Hsu, Y.C., 2000. "Mulit-hop cellular: a new architecture for wireless communications", Proceedings of IEEE INFOCOM 2000, pp. 1273–1282.

Luo, H. and Lu, S. 2000. “Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks”, Technical Report TR-2000.

Luo, H., et al. 2002. “Self-Securing Ad Hoc Wireless Networks”, in IEEE symposium on computers and communications, Taormina-Giardini Naxos, Italy: IEEE Computer Society.

Narasimha, M., G. Tsudik, and J.H. Yi. 2003. “On the utility of distributed cryptography in P2P and MANETs”: the case of membership control, in Network Protocols, Proceedings, 11th IEEE International Conference on.

Ngai, E.C.H. and M.R. Lyu. 2004. “Trust- and clustering-based authentication services in mobile ad hoc networks”, in Distributed Computing Systems Workshops, Proceedings. 24th International Conference.

Schneier, B. 1996. “Applied Cryptography”, 2nd Edition, John Wiley & Sons, ISBN 0-471-11709-9.

Shamir, A. 1979. “How to Share a Secret”, Communication of the ACM 22, No.11, 612-613.

Stallings, W. 2003. “Cryptography and Network Security: Principles And Practices”, 3rd Edition, Prentice Hall, ISBN: 0-13-091429-0.

“The Network Simulator- NS-2”, Home page, http://www.isi.edu/nsnam/ns/, last visited 1st March 2007.

Wu, H et al, 1994. "Integrated cellular and ad hoc relaying systems: iCAR", IEEE Journal on Selected Areas in Communications 19 (10) (2001) 2105–2115.

Xu, G. and Liviu, I. 2004. “Locality Driven Key Management Architecture for Mobile Ad-hoc Networks”, Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference, 25-27, pp: 436 – 446.

Yi, S. and Kravets, R. 2003. “MOCA: Mobile Certificate Authority for wireless ad hoc networks, In proceedings of the 2nd Annual PKI Research Workshop (PKI 03).

Zhou, L. and Z.J. Haas. 1999. “Securing ad hoc networks” Network, IEEE, 1999. 13(6): p. 24-30.

Zimmermann, P. R. 1995. “The official PGP user's guide”, Cambridge, Mass ; London: MIT Press. xviii, 127p.