Predictive Preemptive Certificate Transfer in Cluster-Based Certificate Chain

Boukli-Hacene Sofiane[1], Ouali abdelkader[2], Bassou Asmaa[1]

[1] Evolutionary Engineering & Distributed Information Systems Laboratory EEDIS
Computer science department, Djillali Liabes University at Sidi bel abbes , Sidi Bel Abbes , Algeria
[2] Computer science and information technology of Oran Laboratory LITIO
Computer science department, Es-senia, Oran University , Oran , Algeria
boukli@gmail.com, oualiaek@hotmail.fr, blue_simsim@hotmail.fr

Abstract: Mobile ad hoc networks are a set of nodes that cooperate and communicate wirelessly. This kind of networks in easy to deploy because there is no need of any pre-existing infrastructure. Security in MANETs is a very important issue and it is hard to use conventional security techniques. Many approaches have been proposed to secure communication in MANETs; most of them are based of public-key certifications which create a multitude of trust communication model.

In this paper, we propose an amelioration of a distributed certificate chain that relies on the cluster based routing protocol. In our scheme, after forming clusters, the cluster-head node issue certificates for other nodes within its cluster. When a member node want migrates to an adjacent cluster, the cluster-head sends the node's certificate to surrounding cluster-heads via gateway nodes. The protocol was equipped by a preemptive predictive module to predict migration intention of member nodes. This approach has been evaluated by detailed simulation study. Simulation results show that this approach is scalable and generate lower certification overhead.

Keywords: DPKI, Certification chain, predictive preemptive routing, certification Migration, CBRP**.**

1 Introduction

Mobile ad hoc network (MANETs) is a collection of wireless nodes that dynamically organize themselves in an arbitrary network topology. Nodes within MANETs cooperate to deliver data packets to their destination using a routing protocol. Many routing protocols that respect MANETs characteristics have been proposed in literature [1-6]. Several modifications have been proposed in order to ameliorate the performance of these protocols and to consider other issues such as security [7-10].

The dynamic nature of MANETs makes them highly vulnerable to various security threats. To improve security within MANETs, several approaches have been proposed; most of them are based of public-key infrastructure (PKI) which creates a multitude of trust based communication model. Certificate authority (CA) is a trusted-by-all party used for managing public-key user certificates (PKC). It is one of the most important components of PKI infrastructure. The trivial approach to implement a CA is to centralize CA task in a single node within MANETs. This traditional approach has many problems that are detailed in [7].

Hahn et al have proposed a practical model distributed CA (DCA) approach of PKI relying on the cluster based routing protocol (CBRP) [11]. Cluster-heads functions as CA and issues certificates in a distributed fashion. The certificates are chained effectively and the signed messages can be transferred over a certificate chain.

This paper presents an enhancement of PKI based on DCA over CBRP routing protocol proposed by Hahn et al [11]. CBRP has been equipped with a predictive preemptive mechanism [12-14]. Originally, predictive preemptive was proposed to anticipate link failure in AODV. In this work, the extension is used to predict node migration to adjacent clusters. When the cluster-head node predicts that a member node wants migrate to an adjacent cluster, it sends the node's certificate to surrounding cluster-heads via gateway nodes.

The rest of the paper is organized as follows. In the next section, we present briefly CBRP routing protocol. In Section 3, we discuss how trust can be initially established and maintained between the nodes of a MANET and exhaustively survey related work. We detail the amelioration of the work of Hahn et al [11], by extending CBRP using predictive preemptive module and the repercussions of this enhancement on the certificate management process in section 4. In Section 5, we compare this solution with the related work using a detailed simulation study. Finally, Section 6 concludes the paper and gives some perspectives.

2 Cluster-based routing protocol

The architecture of ad hoc networks can be classified into hierarchic and flat architecture [1, 15] depending on routing protocols. CBRP is one of the well known hierarchical routing protocols. In CBRP, network is divided into a number of overlapping clusters whose union covers the entire network. HELLO packets sent from neighboring nodes are used to form 2 hops diameter clusters in a distributed way. The membership in each cluster changes over time depending on the mobility of nodes. Within each cluster, one node is elected to perform the function of a cluster-head [16, 17]. The lowest ID clustering algorithm is used to elect the cluster-head. This technique consists of selecting the node with the lowest ID among its neighbors to act as cluster-head. The cluster-head keeps cluster membership information in its neighbor table and 2 hops topology database, also; it maintains a cluster adjacency table to communicate with neighboring cluster-heads. Communication between two nodes that are in two different clusters is done through an inter cluster communication. An inter cluster route is created using a source routing protocol such as DSR[2, 3]. Only cluster-heads are able to generate routing packets: Route Request (RREQ) and Route Reply packets (RREP). A RREQ is sent by source node to discover a route to a destination, and RREP is the response of RREQ from a destination. Gateway nodes are responsible for data and routing packets forwarding and broadcasting any new topology information.

3 Distributed Certificate Authority in MANETs

Public-key infrastructure (PKI) is one of the important security mechanisms in wired and wireless networks. Communicating entities in PKI must detain a public and private key pair. This pair is generated by a trusted-by-all authority, called certificate authority (CA). The CA issues and signs a public-key certificate (PKC) for entities using its private key. It is also responsible for revoking, updating and renewing PKC.

The trivial approach to implement a CA is to centralize its function into a single node. This technique faces many problems such as CA availability because of MANET characteristics [18]. The dynamic nature and the absence of a fixed infrastructure compromise the network operation due to CA movement outside of network coverage. Distributed certificate authority (DCA) techniques have been proposed to remedy the problem of CA availability. DCA consists of distributing the CA's private key to a number of shareholding DCA nodes. The public-key of the DCA will be known by all nodes within the network and will be used to verify signatures of certificates issued by the DCA.

Two categories of DCA approach have been proposed: fully and partially distributed certificate authorities. In one hand, in fully distributed certificate authorities (FDCA) all nodes within a network function as CA and each of them generates partial certificates [19-22]. These techniques are reputed by the improvement of the availability and reducing the communication delay. Although, in order to identify and isolate any misbehaving or compromised nodes, these schemas require the use of an intrusion-detection system. On the other hand, the CA function is distributed over a set of special nodes using a secret sharing in partially distributed certificate authorities (PDCA). CA nodes are characterized by high energy level and can be adapted to the heterogeneity of network nodes. Each of them can generate partial certificates, and client nodes combine certificates to get a valid one.

3.1 Partially Distributed Certificate Authority

Zhou and Hass [7] proposed to distribute the services of CA using (k, n) threshold cryptography (fig. 1). In this approach, Each CA generates a portion of the certificate using its share and sends it to a special node that is designated as a combining node. The combiner node collects partial certificates and computes a valid certificate for client node. However, it is always possible for a combining node to be compromised by an adversary or be unavailable due to the exhaustion of the battery or poor connectivity. As a solution, authors proposed selecting a sub set of DCA nodes as combiners, to ensure that at least one combiner can successfully reconstruct the digital signature. The authors have not paid too much importance to the certificate revocation; they proposed a simple approach which is a certification revocation list (CRL). Yi and Kravets extended this approach [23] and Bechler applied it to a large-scale MANET, in which the network is divided into many clusters [24]. The cluster-heads form the DCA and provide certificate service to cluster members.

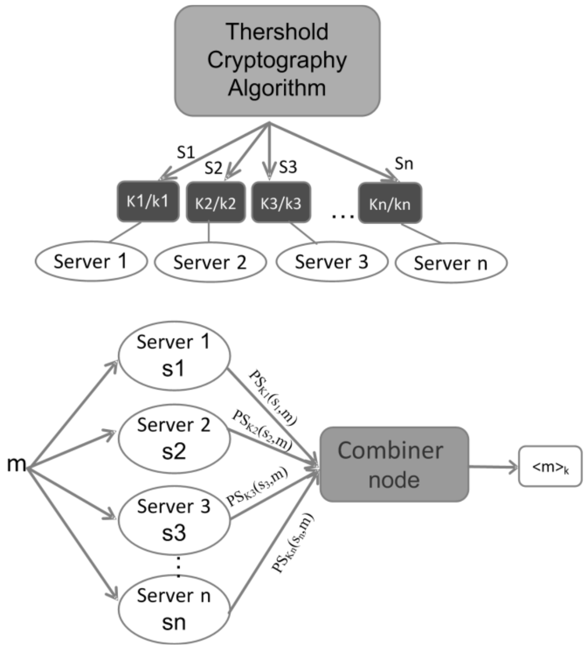

Figure1. (k, n) Thershold cryptography configuration

Yi et Kravets [23] proposed a MObile Certificate Authority (MOCA) using (k, n) threshold cryptography. This approach differs from the original proposal of Zhou and Hass [7], since it does not require a combining node to calculate a signature. The combination of signature portions is performed by the node that requests a certification. This proposal focuses on one-to-many-to-one communication pattern between a node and MOCA. MOCA certification protocol allows a node requesting certification services to broadcast certification request packets (CREQ). Any MOCA node that receives CREQ responds with certification reply (CREP) containing its partial signature. If the node successfully receives valid CREP from a subset of MOCA within a timeout, it can reconstruct the full certificate; else, it must launch a new certification discovery. This method is suitable for flat routing protocol in MANET such as AODV [4-6, 25], DSR [2, 3].

To revoke a certificate, all MOCA nodes must agree. Each MOCA node generates a signed partial revocation certificate that contains its own information and broadcast it through the network. Any node that collects k or more such partially signed revocation certificates can reconstruct the full revocation certificate. The list of revoked certificates or the CRL can be maintained by any node in the network since revocation certificates are not secrets but public information.

These previous approaches assume that public-key pairs are issued and distributed before network creation. This assumption makes the system totally unsuited for self-organized MANET because all certificates must be known by the DCA servers before providing any access to certification services, in addition to the high communication overhead caused by flooding.

4 Certificate Chains

Hubaux et al [26] proposed a very practical scheme for self-organizing MANET. In their approach, there is no concept of CA and every node acts as its own CA, similar to the Pretty Good Privacy (PGP) [27-29]. Each node sends its own certificate to other nodes and maintains a limited certificate directory composed certified neighboring nodes. The main difference with PGP is that there is no centralized certificate management, and every node stores a part of the certificate directory in self-organized nature. Key authentication between nodes is performed by finding an intersecting point between the certificate directories carried by nodes to form a web of trust. Figure 2 presents the formation of a trusted path.

The user can revoke any certificate issued to other users if they lose their trust in the public-key / identity. Similarly, users can also revoke their own certificate if they believe that their private key has been compromised.

Capkun et al [30] proposed an explicit and implicit revocation scheme. In one hand, the implicit scheme is based on revocation timeout certificates. This model assumes that users exchange updated version of the certificate during communication within a timeout. On the other hand, users who usually request certificates from the revocation node, send an explicit revocation message to its neighboring nodes.

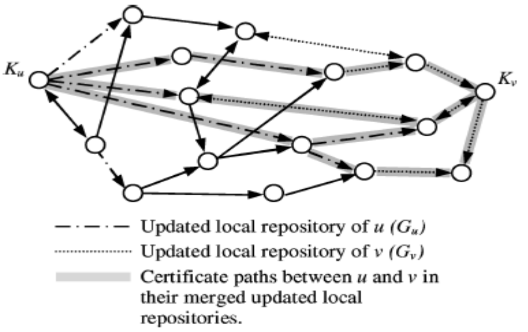
K_u
K_v
Updated local repository of u (G_u)
Updated local repository of v (G_v)
Certificate paths between u and v in their merged updated local repositories.

Figure 2. Certificate path between node u and node v

This scheme suffers from the delay and the large amount of traffic required to collect certificates. Furthermore, there is no definite trust anchor like the CA in other CA-based PKI approaches.

A modified version of [30] is proposed in [31]. In this version, all nodes authenticate themselves via certificate chains in a fully distributed system. The authors introduce a bootstrap server in order to initialize the system. This server distributes to each node a list containing pairs of identifiers and public-keys, and each node generates the corresponding certificates.

4.1 Cluster-Based Certificate Chain

Hahn et al [11] proposed an improvement of key management by combining certificate chaining and cluster-based CBRP routing protocol. In this approach, authors take advantage of the protocol's routing data in order to create a web of trust. They assume that all nodes detain a public/private key peer and Cluster-head acts as CA. The cluster-head is elected using the lowest ID algorithm and the certificate chaining is used only if there is an inter-cluster communication via gateway nodes.

CBRP data structures have been enriched by certificate cache table and CRL (certificate revocation list). The certificate cache of each node stores the certificates of its communication nodes. Certificate cache entry includes the node identity and certificate. The CRL contains the list of revoked certificates, where each entry includes the ID of a node with a repealed certificate and the serial number of the certificate.

The certificate agreement is done after cluster formation, and each node can obtain a certificate from cluster-head. The cluster-head issues a certificate in order to sign cluster members public-key, and the certificate is then stored in the certificate cache.

The gateways issue a certificate to sign Cluster-head's public-key and adjacent cluster gateways public-key. This certificate is stored in the gateway node. The certificate is issued in the following cases, when:

- A node requests a certificate after a cluster is formed
- A node requests a certificate as it moves to adjacent cluster
- After a certificate revocation

The figure below illustrates certificate issuing.

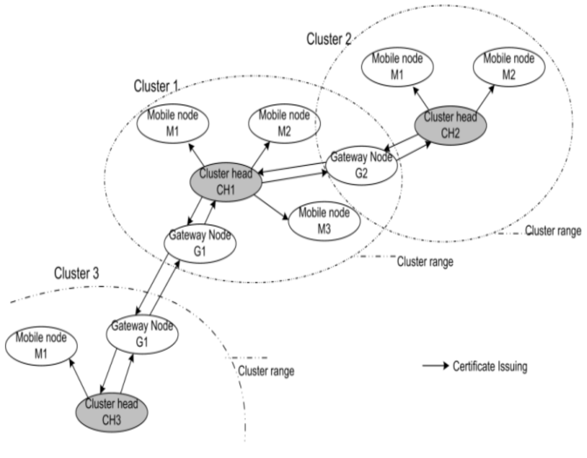

Figure 3. Certificate issuing

When a certificate expires, a new certificate must be issued and sent to the node with an expired certificate. This is similar to the generation of the certificate. The difference is that the expired certificate must be sent to the Cluster-head and verified in order to get a new one. The incoming figure shows certificate renewal process.

Depending on the check outcome, a node may obtain a new certificate or not. A node can renew its certificate only if the detained expired certificate is legal, and it does not leave the current cluster, otherwise; the certificate cannot be renewed.

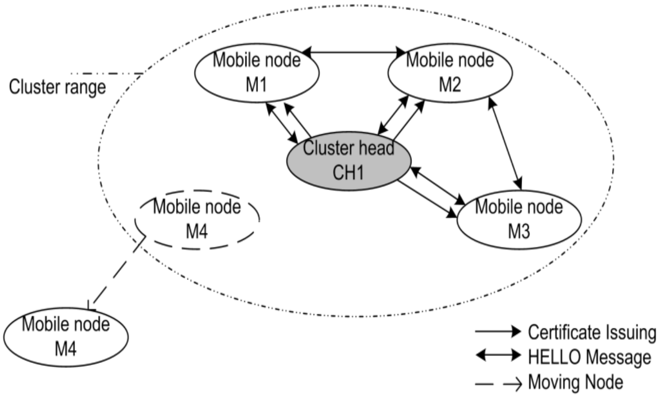

Figure 4. Certificate renewing

This approach generates lower certificate maintenance overhead by resolving certificate transaction problems. Chaining is done only with trusted nodes that are Cluster-head and gateways, unlike PGP model in which the transaction is made using all the network nodes, thereby, increasing the certificates overhead and the risk of a compromised node in the chain of certificates. Moreover, chaining is done in one direction and all certificates of intermediate nodes are stacked linearly, which causes a very significant overhead.

However, key management in [11] is not quite optimal. When a node leaves the cluster, it should always request a new certificate which may increase the overhead and consumes more energy, besides that, the node behavior is not tractable, which prevents check whether this node already has a malicious behavior or not.

Certificates Renewal is also a problem since only the cluster-head that issued the certificate may renew it. If a certification expires during node transition to another cluster, the node must request a new certificate from the destination Cluster-head; however, due to the dynamic nature of MANET, it is more judicious to renew certificates than generating new ones.

5 Our approach

Hahn et al [11] studied a cluster model based on PKI for MANET where cluster-heads acts as virtual CA and issue certificates for cluster members. The certificate chain built in this system allows the exchange of session keys to encrypt / decrypt data being transferred. However, due to MANET characteristics such as mobility, a node always requests a new certificate from a cluster-head when it moves between clusters, which overload the cluster-head.

The idea is to ensure that when the member intends to leave the cluster, information is disseminated through gateways to adjacent cluster and report a possible arrival of the member. In this part, we develop our approach in which we enhance the work done in [11] with prediction preemption [12-14], in order to address the problem of availability and renewal of certificates.

In this work, we consider that the coverage area of a cluster-head which form the cluster is divided into two regions, a safe region where a mobile node is near to the cluster-head and is not likely to disconnect, and the other uncertain or preemption. A node is considered in a preemptive region if the signal strength of a received packet from its cluster-head is below a threshold power Pt. When a node enters this area, at least, three consecutive measurements of packets signal strength are done, and the Lagrange interpolation is used to predict communication link failure. The general form of this interpolation is:

$$y = \sum_{i=0}^{n} \left[\frac{\prod_{\substack{j=0 \\ j\neq 0}}^{n} \left(x - x_j\right)}{\prod_{\substack{j=0 \\ j\neq 0}}^{n} \left(x_i - x_j\right)} \times y_i \right] \qquad (1)$$

We store the power strengths of the three signals and their times of occurrence. When two consecutive measurements give the same signal strength, we store the time of the second occurrence. The expected signal strength P of the packets received from the Cluster-head node is computed as follows:

$$P = \left(\frac{(t - t_1)\times(t - t_2)}{(t_0 - t_1)\times(t_0 - t_2)} \times P_0 \right) + \left(\frac{(t - t_0)\times(t - t_2)}{(t_1 - t_0)\times(t_1 - t_2)} \times P_1 \right) \qquad (2)$$
$$+ \left(\frac{(t - t_0)\times(t - t_1)}{(t_2 - t_0)\times(t_2 - t_1)} \times P_2 \right)$$

Where P_0, P_1, P_2 are the measured power strengths at the times t_0, t_1, and t_2, respectively.

The time t is the sum of time required to send the certificate to Cluster neighbors (Inonde_Period) and the difference between t_2 and the average value of the measurement; this value has been determined empirically. That is to say:

$$t = 2 \times t_2 - \left(\frac{t_0 + t_1 + t_2}{3}\right) + Inonde\_period \qquad (3)$$

When P is less than the minimum acceptable power (81 dB) a warning message is sent to the Cluster-head. The Cluster-head sends the certificate to neighboring cluster-head through gateways.

5.1 Data structures

Our scheme requires a new data structure in which the originator cluster-head put the addresses of nodes that will quit their coverage and join an adjacent cluster. When the destination Cluster-head detects the presence of the newcomer node in its scope using the hello packets it sends an alert to the originator cluster-head. Once the originator cluster-head receives the alert message it put the id and the public-key of the transferred node in the data structure.

5.2 The agreement certificates

As we already mentioned, our approach is an improvement of certificates chaining based on clusters [11]. We will keep the same principle cited earlier with some modification.

Certificates are generated either by a Cluster-head or a Gateway to according to the member position in the topology. The following figures show the possible cases to issue a certificate.

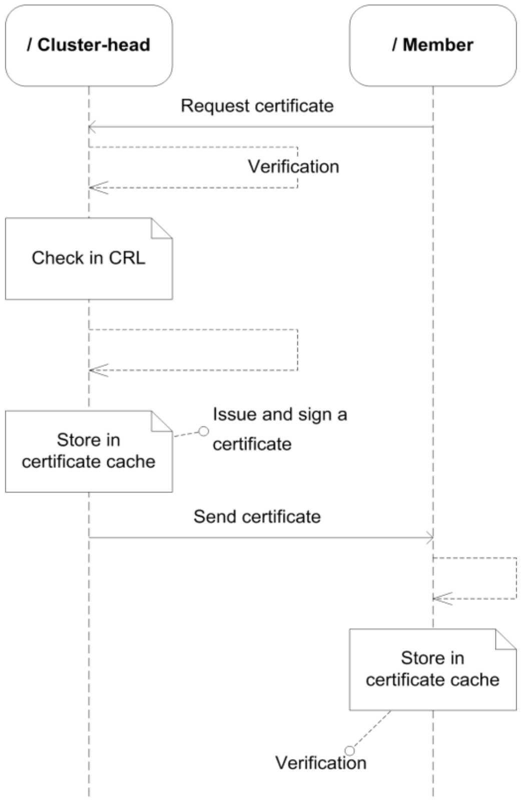

Figure 5. Certificate issuing for a member after cluster forming

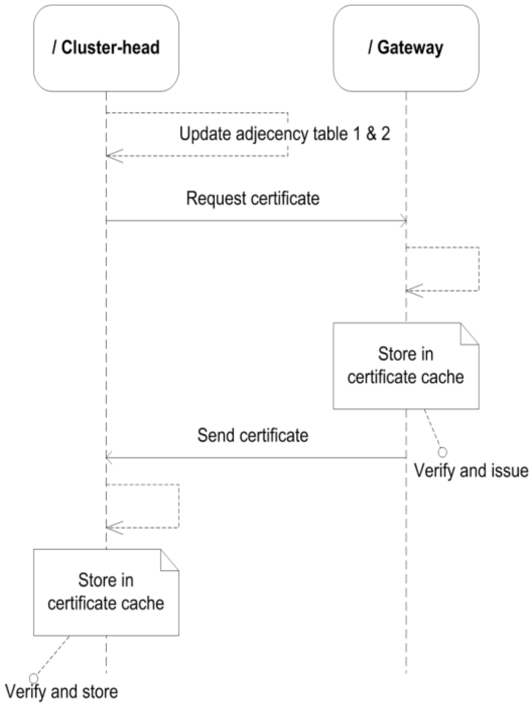

Figure 6. Certificate exchange between a cluster-head and a gateway

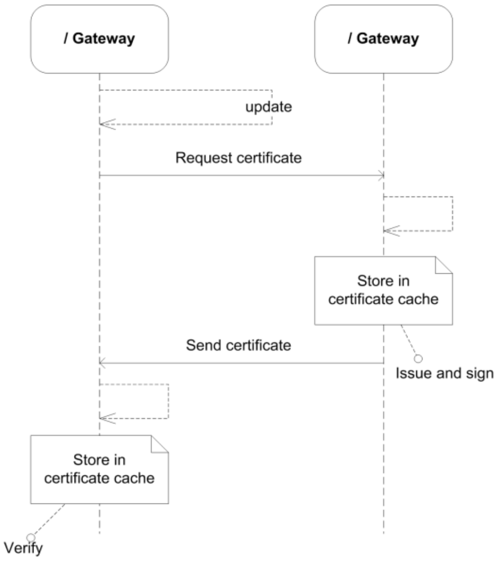

Figure 7. Certificate exchange between Gateways

5.3 Certificate Transfer

The Lagrange interpolation function allows the Cluster-head node to predict whether a member will quit its coverage, if so, the Cluster-head sends the address and the certificate of the corresponding node to all the neighboring Cluster-heads via gateways. Once the node tries to join an adjacent cluster, the Cluster-head compares the node’s address with the received one and saves its certificate without issuing a fresh one. This allows a node to move from one cluster to another without asking each time a new certificate, even if there will be a temporarily link disconnection as shown in Figure below. This enhancement offers a big possibility of certificate renewal even if the node transits to another cluster unlike the solution proposed in [11].

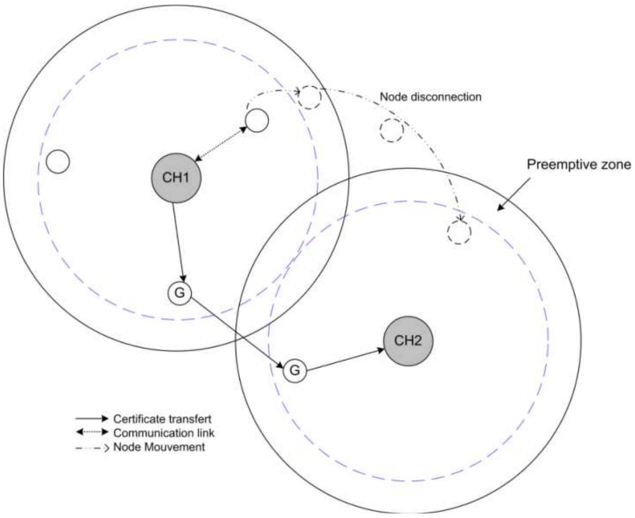

Figure 8. Certificate Transfer

5.4 Certificate renewal and certificate revocation

Renewing certificates is performed when the certificate is expired, and can be done by the cluster-head or neighboring Cluster-heads who have collaborated in a transfer certificate within a fixed period, to avoid overloading of memory of Cluster-heads. Unlike the Cluster-Based Certificate Chain method, a certificate can be revoked anywhere in the network.

6 Performance Evaluation

The performance of the approach described above is simulated and the results are presented in this section.

6.1 Simulation setup

In order to evaluate the performance of the proposed approach and compare it to the original Cluster-Based Certificate Chain [11], We use an extended version of the well known simulator NS-2 [32]. The extension includes CBRP protocol [33], certificate management libraries [34], and predictive preemptive mechanism [35]. The network is composed of 25, 50 and 75 mobile nodes equipped IEEE 802.11 MAC with a transmission range of 250m for 1000s simulation time. These nodes are uniformly deployed within area of 1500m by 300m. The node movement follows the widely used random waypoint model [3] in a free space model with maximal moving speed of 20m/s. We carry out simulations using mobility scenarios generated with five different pause time: 0, 250, 500, 750 and 1000s. A pause time equal to 0s corresponds to a continuous mobility, and 1000s is for limited motion. Constant bit rate (CBR) is used in the simulations with a packet rate of 4 packets/sec. The value of Pt is empirically determined to be equal to -80.64545 dB. Each scenario is repeated 10 times and the average values of the results are computed.

In this study, we are interested by the total of issued certificate (certificate overhead), and we use it as a performance metric.

6.2 Results and discussions

We report the results of the simulation experiments for the original Cluster-Based Certificate Chain and for the Cluster-Based Certificate Chain with predictive preemptive certificate transfer.

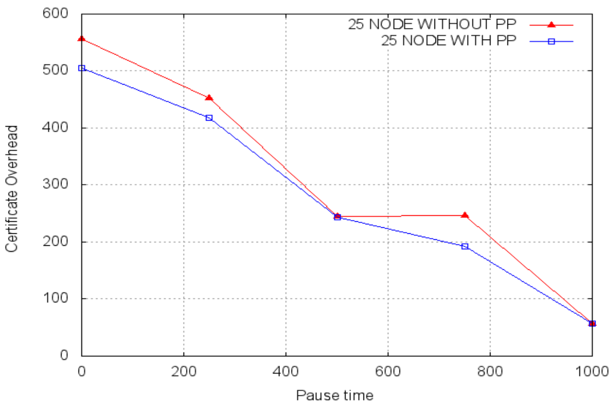

Figure 9. Cluster-Based Certificate Chain with/without predictive preemptive certificate transfer 25 nodes

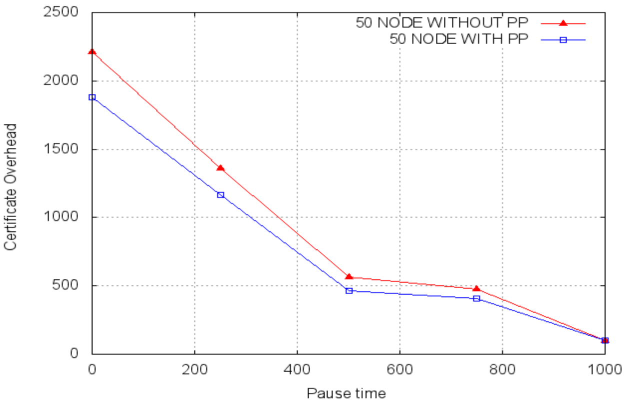

Figure 10. Cluster-Based Certificate Chain with/without predictive preemptive certificate transfer 50 nodes

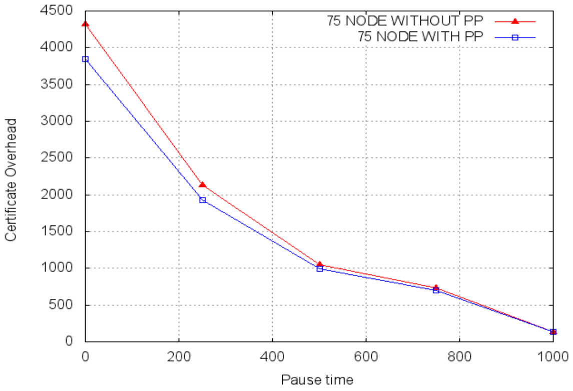

Figure 11. Cluster-Based Certificate Chain with/without predictive preemptive certificate transfer 75 nodes

The figures above show how mobility and number of nodes (node density) affect the certificate overhead

The first observation is that in the case of high node density, the certificate overhead is high because CA should deliver a certificate to each communicating node.

It is noticed from the graphs that, when node motion is low, the overhead is low; furthermore, the two techniques are similar; this is because member nodes stay longer within cluster coverage. In this case, certificate renewal is solicited and there will be no need to issue a new certificate because of node mobility.

It is also observed that the overhead is high when the number of nodes is high, especially with high mobility. This results from the fact that too many nodes request a new certificate from CA and from adjacent CA when a node migrates to a surrounding cluster in the original technique. However, we depict that, our approach outperforms the original with 9.09% to 15.55% less certificates.

In the original approach, nodes request a fresh certificate from CA every time they migrate to a neighboring cluster, which generates a very obvious elevation in the number of certificate even if the number of nodes is small. However, in our approach, the use of prediction / preemption technique allows a CA to predict node movement, and transfer its certificate to adjacent CA. the destination CA trust the newcomer node and do not issue a new certificate. This can have many repercussions on protocol performance, especially energy, which is a very critical resource for this kind of networks. Also, nodes maintain their seniority during the network lifetime, the associated certificate follows the node in every new cluster, which can be useful in seniority based election algorithm, and cluster member don't have to make the first trust in every new cluster, which make our approach more robust.

7 Conclusion

Mobile ad hoc network (MANETs) is constituted of a set of nodes that collaborate to forward packets to their destination relying on a routing protocol. In literature, many routing protocols that meet MANET’s characteristics have been proposed, and several modifications have been made to address issues such as security.

MANETs are vulnerable to various security threats. In order to improve security within MANETs, several approaches have been proposed; most of them are based on distributed public-key infrastructure (DPKI) which creates a multitude of trust based communication model. One of the original contributions is Cluster-Based Certificate Chain.

In this technique, Nodes use a cluster based routing protocol to deliver the data packets to their destinations. Cluster-head nodes act as a certificate authority and issue certificates for cluster members. However, due to mobility, nodes always request a new certificate from a cluster-heads when it moves between clusters, which overload cluster-heads.

In our study, we propose an enhancement to Cluster-Based Certificate Chain by using a predictive preemptive mechanism. This mechanism allows a cluster-head to predict node’s migration plan towards an adjacent cluster. When a cluster-head predicts that a member node will leave its coverage, it sends the node’s certificate to surrounding cluster-head via gateway nodes. Our improvement gives a satisfactory result, where the number of issued certificates has declined by about 15%.

As perspective, we propose to add the predictive preemptive mechanism to gateway nodes in order to send migrating node’s certificate to concerned neighboring cluster-head.the same technique can be used not only to improve the overhead of certificates, but also to detect and repair the link fails, when node transmit data to another node, this can be done using the same functionality of the cluster-heads as well as to control the overhead of certificates and manage the link fails in the network.

References

[1] M. Jiang, J. Li, and Y. C. Tay, "Cluster Based Routing Protocol(CBRP)," Internet Drafts, RFC Editor, 1999.

[2] D. B. Johnson, "Routing in ad hoc networks of mobile hosts," In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pp. 158-163, 1994.

[3] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," T. Imielinski and H. Korth (eds.) in Mobile Computing Boston Academic, pp. 153-181, 1996.

[4] C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," Internet Drafts, RFC Editor, 2003.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing,", Second Ieee Workshop on Mobile Computing Systems and Applications 'Wmcsa '99), pp. 90-100, 1999.

[6] E. M. Belding-Royer and C. E. Perkins, "Evolution and future directions of the ad hoc on-demand distance-vector routing protocol," Ad Hoc Networks, vol. 1 , No. 1 , pp. 125-150, 2003.

[7] L. D. Zhou and J. Z. Hass "Securing ad hoc networks," Ieee Network, vol. 13, pp. 24-30, 1999.

[8] D. Hongmei, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol. 40, pp. 70-75, 2002.

[9] P. Vinayakray-Jani and S. Sanyal, "Security Architecture for Cluster based Ad Hoc Networks," CoRR, vol. abs/1207.1701, 2012.

[10] S. Sahraoui and S. Bouam, "Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks," Communication Networks and Information Security (IJCNIS), Vol. 5, No. 3, pp. 178-185, 2013.

[11] G. Hahn, T. Kwon, S. Kim, and J. Song, "Cluster-Based Certificate Chain for Mobile Ad Hoc Networks," in International Conference on Computational Science and Applications (ICCSA) , pp. 769-778, 2006.

[12] S. Boukli-Hacene, A. Lehireche, and A. Meddahi, "Predictive preemptive ad hoc on-demand distance vector routing," Malaysian Journal of Computer Science, Vol. 19, No. 2, pp. 189-195, 2006.

[13] S. Boukli-Hacene and A. Lehireche, "An Overview On Predictive And Preemptive Maintenance Techniques In MANETs," In Proceedings of Colloque sur l’Optimisation et les Systèmes d’Information(COSI'07), Oran, Algeria, pp. 25-32, 2007.

[14] M. Ali Cherif, M. K. Feraoun, and S. Boukli-Hacene, "Link Quality and MAC-Overhead aware Predictive Preemptive Multipath Routing Protocol for Mobile Ad hoc Networks," Communication Networks and Information Security (IJCNIS), Vol. 5, No. 3, pp. 210-218, 2013.

[15] A. M. Popescu, G. I. Tudorache, B. Peng, and A. H. Kemp, "Surveying Position Based Routing Protocols for Wireless Sensor and Ad-hoc Networks," Communication Networks and Information Security (IJCNIS), Vol. 4, No.1 , pp. 210-218, 2012.

[16] C. R. Lin and M. Gerla, "A distributed architecture for multimedia in dynamic wireless networks," Global Telecommunications Conference (GLOBECOM '95), IEEE, Vol. 2, pp. 1468-1472, 1995.

[17] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," IEEE Journal on Selected Areas in Communications, Vol. 15, pp. 1265-1275, 1995.

[18] L. Zhou, F. B. Schneider, and R. V. Renesse, "COCA: A secure distributed online certification authority," Journal ACM Transactions on Computer Systems (TOCS), Vol. 20, pp. 329-368, 2002.

[19] D. Joshi, K. Namuduri, and R. Pendse, "Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: an analysis," EURASIP Journal of Wireless Commununication Network, Vol. 2005, pp. 579-589, 2005.

[20] S. A. Hosseini Seno, R. Budiarto, and T.-C. Wan, "A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority," Arabian Journal for Science and Engineering, Vol. 36, pp. 245-257, 2011.

[21] H. Y. Luo and S. W. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks," Department of Computer Science, University of California, Los Angeles, Calif, USA, 2000.

[22] H. Y. Luo, P. Zerfos, H. J. Kong, S. W. Lu, and L. X. Zhang, "Self-securing ad hoc wireless networks,": Seventh International Symposium on Computers and Communications (Iscc 2002), pp. 567-574, 2002.

[23] S. Yi and K. R, "MOCA: mobile certificate authority for wireless ad hoc networks," in Proceedings of the Second Annual PKI Research Workshop (PKI 03), 2003.

[24] M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, and L. Wolf, "A clusterbased security architecture for ad hoc networks," in 23rd Conference of IEEE Communication Society (INFOCOM 2004), Hong Kong, China, 2004.

[25] E. M. Royer and C. E. Perkins, "An implementation study of the AODV routing protocol," In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2000), Vol. 3, pp. 1003-1008, 2000.

[26] J.-P. Hubaux, L. Butty, and S. Capkun, "The quest for security in mobile ad hoc networks," In Proceedings of the the 2nd ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, pp. 146-155, 2001.

[27] W. Stallings, "Pretty Good Privacy," Byte, Vol. 19, pp. 193, 1994.

[28] S. Garfinkel, "PGP: Pretty Good Privacy, " O'Reilly and Associates, California, USA, 1995.

[29] P. R. Zimmermann, "The official PGP user's guide" MIT Press, 1995.

[30] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," Ieee Transactions on Mobile Computing, Vol. 2, pp. 52-64, Jan-Mar 2003.

[31] K. Ren, T. Y. Li, Z. G. Wan, F. Bao, R. H. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks," Computer Networks-the International Journal of Computer and Telecommunications Networking, Vol. 45, pp. 687-699, 2004.

[32] ns2 (network simulator 2). Available: http://www.isi.edu/nsnam/ns/

[33] Cluster based routing protocol (CBRP). Available: http://www.comp.nus.edu.sg/~tayyc/cbrp/

[34] A. Ouali, A. Bassou, (2012). Certificate material. Available:http://www-inf.univ-sba.dz/enseign/BOUKLI/key_material.zip

[35] S. Boukli-Hacene. (2006). predictive preemptive ad hoc on demand distance vector (PPAODV). Available: http://www-inf.univ-sba.dz/enseign/BOUKLI/PPAODV.zip