An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks

Rajaram Ayyasamy[1] and Palaniswami Subramani[2]
[1]Electronics and Communication Engineering Department, Karpagam College of Engineering, Anna University Coimbatore, India
[2]Government College of Engineering, Bargur, India

Abstract: *In Mobile Ad-hoc Networks (MANETs), it is easy to launch wormhole, man-in-the-middle and Denial of Service (DoS) attacks, or to impersonate another node. Our previous work established a network consisting confidentiality and authentication of packets in both routing and link layers. As an extension to our previous work, in this paper, we propose to develop an enhanced distributed certificate authority scheme to provide data integrity, thus making the network more secure from both inside and outside attacks. The proposed scheme makes use of Shamir's secret sharing scheme along with a redundancy technique to support certificate renewal and revocation. The malicious nodes are detected by the trusting mechanism by monitoring the behavior hop by hop. By simulation results, we show that the proposed scheme achieves more packet delivery ratio while attaining less delay and overhead, compared with the previous existing scheme.*

Keywords: *Shamir's secret sharing, DoS, routing cum forwarding, certificate revocation, certification revival.*

Received May 3, 2010; accepted August 10, 2010

1. Introduction

1.1. Mobile Ad-hoc Network (MANET)

MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. The mobility of the routers are provided randomly and organized themselves arbitrarily; thus, the network's wireless topology may alter rapidly and unpredictably [8]. These types of networks function in the absence of any fixed infrastructure, which provides easy deployment [7]. However, due to the lack of any fixed infrastructure, it becomes complicated to exploit the present routing techniques for network services, and this provides some huge challenges in providing the security of the communication, which is not done effortlessly as the number of demands of network security conflict with the demands of mobile networks, largely due to the nature of the mobile devices (e.g., low power consumption, low processing load) [13].

MANET has various potential applications, which are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers [3]. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

1.2. Threats in MANET

The broadcasting nature of transmission and the nodes self routing environment opens up the perception of security in MANET. The security issue of MANET is of large concern taking into account its various factors like its open network, mobility factor and other factors. When taking into security aspects, the attacks on MANET can be classified into two; internal attacks and external attacks [2, 5, 10, 18]. Internal attacks are those attacks which are caused by inside node of a network. These attacks are produced by either malicious nodes or by selfish nodes inside a network. These internal attacks are tough to detect as nodes affected by such an attack generate themselves the valid signatures using their private keys. Examples of internal attack are internal eavesdropping, where the nodes extracts copy of all information and exploited it without the knowledge of other nodes and packet dropping.

In external attacks, the attackers are from outside the network but cause damage or compromises network within the network. Attacks from external nodes can be prevented from cryptographic techniques such as encryption and authentication. As per routing, external attacks can be divided into active and passive attacks. Active external attacks use to degrade or stops message flow between the nodes. Denial of Service (DoS) attacks, packet dropping or flooding of packets are some examples of active external attacks. Passive external attacks are formally done by compromising the nodes and extracting vital information of the network. In passive attack, the attacker does not disrupt the network operation but only extracts information to damage further network operation. These type of attacks are basically impossible to detect, thus making it hard to produce security for such attacks.

1.3. Security Challenges in MANET

The nature of MANET makes it vulnerable to attacks. Challenges in MANET securities are discussed briefly [3].

- *Availability*: Should withstand survivability regardless of DoS attacks like in physical and media access control layer attacker uses jamming techniques for hinder with communication on physical channel. On network layer the attacker can interrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g., key management service.
- *Confidentiality*: Should safeguard certain information which is not to be disclosed to unauthorized entities.
- *Integrity*: Transmitted Message should be genuine and should never be corrupted.
- *Authentication*: Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes.
- *Non-Repudiation*: Safeguards that the source of a data should not reject having sent the data.

1.4. Problem Identification and Proposed Solution

In Mobile Ad-hoc Networks (MANETs), it is simple to launch wormhole, man-in-the-middle and DoS attacks, or to impersonate another node. To resist against such attacks from outsider nodes, we propose a hop-by-hop authentication protocol. It authenticates packets at every hop by using a Certificate Authority (CA) based approach and drops any packets that originate from outsiders. Each node monitors and evaluates the behavior of its successors by itself, and as soon as it accuses a node it launches a procedure to approve this accusation. In our previous work [11], we have analyzed about the confidentiality and authentication of data in MANET environment. In this paper, we analyze the integrity of data along with the external attack.

2. Related Work

Akbani *et al.* [1], have proposed a hop-by-hop, proficient authentication protocol, called HEAP. It authenticates packets at each hop using a modified HMAC-based algorithm including two keys and drops any packets that are initialized from outsiders. The method used here can be appropriate for all application like multicast, unicast or broadcast applications. Discovering an insider attack using this protocol is highly improbable. But if a third party Intrusion Detection System (IDS) happens to detect a compromised insider node and raise an alarm to other nodes, HEAP will offer a framework for an effective response system.

Wenbo *et al.* [16], have proposed a self-contained public key-management scheme, a Scalable Means of Cryptographic Key management (SMoCK), which acquires negligible communication overhead for authentication, and offers maximum service availability. Here a combinatorial design of public-private key pairs is created which provides each node with extra protection of more than one key pair to encrypt and decrypt messages. This format helps in earning higher stability in terms of nodes and storage space. The scheme also achieves controllable resilience against node compromise by defining required benchmark resilience.

Saxena *et al.* [9], have discussed about various signature scheme and have studied about the various techniques used. Here they tried the threshold in constructing decentralized access control mechanisms for ad hoc groups. They tried to first, point out the drawbacks of known threshold RSA signatures and tried to build access control mechanisms based on a variety of flavors of distinct logarithm based threshold signatures in this paper they tried to implement three access control mechanisms based on discrete-logarithm based threshold signatures, Threshold DSA (TS-DSA), Threshold Schnorr (TS-Sch) and Threshold BLS (TS-BLS).

Komninos *et al.* [6], have proposed a two-phase detection procedure of nodes that are not authorized for specific services and nodes that have been compromised during their operation in MANET. The detection framework' is enabled with the major operations of Ad-hoc networking, which are found at the link and network layers. The proposed framework is based on zero knowledge techniques, which are particularly designed to achieve node identification but do not rely on symmetric or asymmetric encryption algorithms, digital signatures, sequence numbers and timestamps. The zero knowledge techniques are presented through proofs.

Vaidya *et al.* [15], have put forward AODV with Multiple Alternative Paths (AODV-MAP) scheme and its security extension SAODV-MAP scheme. AODV-MAP scheme is robust and efficient multipath Ad-hoc routing protocol. It was intended to have secured AODV-MAP in order to provide security against various attacks. Security analysis shows that SAODV-MAP is much more robust against various known adversaries than SRP. The simulation results show that SAODV-MAP is better than AODV and as efficient as AODV-MAP in discovering and maintaining routes. Overall, in presence of various malicious nodes, SAODV-MAP scheme outperforms SRP scheme in all of the performance metrics that we examined.

In our previous work [11] we present a solution for node selfishness to attain confidentiality and authentication of packets in both routing and link layers of MANETs. The technique is a double phase; one for detecting and isolating the malicious nodes using the routing layer information and second phase is for link-layer security. For detecting and isolating the malicious nodes we use the packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. this provides an efficient and more secure protocol, as we use only nodes which are stored in the current route need to perform this cryptographic computation as well as authentication is performed for route reply operation. For link-layer security, in the next phase, we use CBC-X mode of authentication and encryption.

Shafiullah *et al.* [12] have proposed a new framework of intrusion detection systems exclusively for wireless mesh networks. That paper served as a baseline guide for investigating intrusion detection systems for large scale multi-hop wireless broadband networks.

3. Proposed Scheme

In the paper, we add integrity factor into our work to secure the network. We provide a certificate authority scheme and increase the security to tackle both internal and external attacks. Our scheme is contributed with three components.

- Monitoring Routing Cum Forwarding (RCF) behavior.
- Certificate revival.
- Certificate revocation.

RCF behavior which is based on our previous work, involves detecting misbehaviors in both the routing as well as the packet forwarding in the network. Certificate revival uses a redundancy scheme [4], in which a node is allocated more than one key share by incorporating redundancy into the network. This mechanism guarantees that genuine nodes can continue to stay in the network by revival of their certificates along a periodical time period. Certificate revocation provides the authority to isolate any malicious nodes or regain the nodes which turn up to its best state after any attack or failure. Thus, Certificate revival and Certificate revocation added to our previous work brings forth the integrity factor along with confidentiality and authentication.

3.1. Monitoring: Routing Cum Packet Forwarding (RCF) Behavior

Monitoring of routing packets and forwarding packets are done using our previous work of Trust based packet forwarding scheme by punishing or rewarding the nodes with decreasing or increasing a trust counter. Each intermediate node marks the packets by adding its hash value and forwards the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, other wise it is decremented. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious.

Before proposing the modification, we can analyze how the trust based packet forwarding scheme works from our previous work.

Each node keeps track of the number of packets it has forwarded through a route using a Forward Counter (FC). Each time, when node n_k receives a packet from a node n_i, then n_k increases the forward counter of node n_i.

$$FCn_i = FCn_i + 1, \quad i = 1,2,\cdots \tag{1}$$

The incremental value, saved in a data structure called Neighbor's Trust Counter Table (NTT), of node n_k is modified with the values of FCn_i.

Similarly each node determines its NTT and finally the packets reach the destination D.

When the destination D receives the accumulated RREQ message, it measures the number of packets received Prec. Then it constructs a MAC on Prec with the key shared by the sender and the destination. The RREP contains the source and destination ids, The MAC of Prec, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route R1. Each intermediate node along the reverse route from D to S checks the RREP packet to compute success ratio as,

$$SRi = \frac{FCni}{\mathrm{Prec}} \tag{2}$$

Where Prec is the number of packets received at D in time interval $t1$. The FCn_i values of n_i can be got from the corresponding NTT of the node. The success ratio value SR_i is then added with the RREP packet. For any node n_k, if SR_k is either minimum or maximum than $SR\min$ (where $SR\min$ is the minimum threshold value) the trust counter value is further decreased or increased respectively.

The incentive value provided to each successful node helps in determining the trustworthiness of the node and shows the misbehaving nodes apart from the network.

To increase the integrity of these forward packets we introduce certification revival scheme using redundancy of [16] to guarantee that genuine nodes can continue to stay in the network by revival of their certificates along a periodical time period.

3.2. Certification Revival Scheme

To communicate between the nodes inside the network, every legitimate node carries a certificate, issued by an offline CA. The certificate comprises of 3 basic fields: Node ID (NID), Initiation Time (IT) and Expiry Time (ET). For CA, we use the concept of secret sharing based upon Shamir's "secret sharing model" [14, 17] with the use of redundancy. Shamir's secret sharing scheme provides security as well as is extendable and flexible. Along with redundancy the mobility factors of Ad-hoc network becomes less concerned.

3.2.1. Shamir's Secret Sharing Model

The CA key is shared to a set of nodes using the Shamir's secret sharing model. Using the model we provide secrecy among a set of nodes from N nodes such that at least k nodes are needed to reconstruct the secrecy among the nodes. Consider the set of nodes be $P1, P2, P3, \cdots, Pn$. Under such condition we follow the following steps:

- *Step 1*: Dealer D constructs polynomial *f(x)* of degree *(k-1)*:

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{k-1}x^{k-1} \tag{3}$$

  Polynomial *f(x)* is constructed over finite field, then $a_0 = \sec ret(s)$. All other coefficients are random elements in the field.

- *Step 2*: Dealer D chooses n random distinct evaluation points: $X_j \neq 0$, and secretly distributes to each participants P_j the share:

$$sharej(s) = (X_j, f(X_j)), \quad j = 1, 2, \cdots, n \tag{4}$$

  The above two steps provides a sharing key among subset of k shares out of n shares. To reconstruct the sharing, the model uses Lagrange interpolation.

- *Step 3*: Using the Lagrange interpolation the unique polynomial $f(x)$ such that degree $f(x) < k$ and $f(j) = sharej(s) \;\; for \;\; j = 1, 2, \cdots, k$:

$$f(x) = \sum_{i=1}^{k} f(i) * Li(X) \tag{5}$$

Where $Li(X)$ is the Lagrange polynomial.

$$Li(X) = \frac{\prod j \neq i(x - xj)}{\prod j \neq i(xi - xj)}. \tag{6}$$

We evaluate the above steps using an example for sharing and reconstructing the CA among the sets of nodes. Consider an example where $n = 6$, are the participant nodes, secret $s = 1234$, then as per the polynomial equation 2 we have,

$$f(x) = a_0 + a_1x + a_2x^2 \tag{7}$$

By taking a random value a_1 and a_2 as 166 and 94, we get the equation as:

$$f(x) = 1234 + 166x + 94x^2 \tag{8}$$

Computing the above equation and distributing the above equation, we are provided with 6 points as (1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614). This provides the sharing values for each node of the sets. We recreate the secret, if at least 3 nodes are present. Let us consider we have 3 random nodes, (x_0y_0)=(2,1942); (x_1y_1)=(4,3402); (x_2y_2)=(5,4414). Using the above equations 5 and 6 we get the same polynomial value as equation 8:

$$f(x) = 94x^2 + 166x + 1234 = f(x) = 1234 + 166x + 94x^2 \tag{9}$$

3.2.2. Modified Sharing Scheme with Redundancy

Deepti *et al.* [4], have modified Shamir's secret sharing works by introducing witness to each node along with adding redundancy. We add this modified technique in our Certification revival scheme. This scheme helps in reconstructing shared keys even if the minimum set of necessary key (k) is not available during reconstruction. For this we provide q shares of value to each node against the traditional value which is 1 shared value for each node.

Increasing the number of shares per node increases the chance of the node recreating the CA key even if the neighboring nodes are less than k. Hence the total number of nodes requisite to recreate the CA key can be less than *(k-1)*, as any node trying to recreate the CA key can get the k required shares from less than *(k-1)* nodes. As the number of shares per node increases, the number of nodes needed to recreate the CA key is descendent.

The probability value for recreating such a scenario is given below. It is estimated that maximum the value of k available, maximum the success rate will be. We consider from the above example, if one of the values (from $k = 3$) moves away, then the existing value will be 2 nodes available to recreate the sharing value. Under such circumstances, the redundant value provides the necessary non-available value to recreate the sharing values.

To calculate the total number of ways $(f(y+\lambda))$ in which the CA key can be recreated, consider the number of ways in which the key shares can be distributed among y nodes such that we have $y, y+1, y+2, \cdots, n$ distinct keys. The number of ways $(y+\lambda)$ key shares can be gathered from y neighbors is given by

$$f(y+\lambda) = a*b*c*d \tag{10}$$

Where,

- a= the number of ways $(y+\lambda)$ keys can be selected from n keys, given by $(nCy+\lambda)$.
- b= the number of ways y keys can be selected from $(y+\lambda)$ keys, given by $((y+\lambda)Cy)$.
- c= the number of ways these y shares can be allocated to the y nodes, given by $(y!)$.
- d= the number of ways in which the remaining shares can be allocated to the y nodes, given by $((y+\lambda-1)Cq-1)^{y}$.

The probability of recreating the CA key given y neighbors is given by:

$$P(y) = \begin{cases} \dfrac{\sum_{\lambda=k-y}^{n-y} \mathrm{f}\,(\mathrm{y}+\lambda\;)}{\sum_{\lambda=0}^{\mathrm{n-y}} \mathrm{f}\,(\mathrm{y}+\lambda\;)} & if\,(y*q) \geq n, \\ \dfrac{\sum_{\lambda=k-y}^{\mathrm{y*q-y}} \mathrm{f}\,(\mathrm{y}+\lambda)}{\sum_{\lambda=0}^{\mathrm{y*q-y}} \mathrm{f}\,(\mathrm{y}+\lambda)} & if\,(y*q) < n, \end{cases} \tag{11}$$

The above equation also takes into account the maximum number of distinct key shares a legitimate node can gather from a coalition of y nodes, which is either $(y \cdot q)$, where q is the number of shares per node, or n depending on whether $(y \cdot q)$ is greater than or equal to n or less than n.

3.3.Certification Revocation Scheme

In our previous work, we increase and decrease a trust counter depending on the behavior of the node. These trust values are saved in NTT where nodes which have trust value lower than the threshold trust value $TCthr$ are termed as malicious. In the certificate revocation scheme, when the node's "Expiry time" (ET) elapsed, the node broadcasts a renewal request packet (RWREQ) to its neighbors. Node which receives a RWREQ, checks its node status from the NTT. If the nodes have value less than the $TCthr$ value, then the RWREQ is dropped or else the node sends a Renewal Reply Packet (RWREP), along with a new IT and ET field, back to the node. Due to the redundancy technique, the renewal of nodes does not consume time or halts, even if any movement of nodes or node failure or even disconnection in network occurs.

Thus our work increases the integrity factor of the data in the network due to certificate authority scheme along with resisting against the outside attackers. Our scheme also reduces the overhead of nodes because of the redundancy factor, as it reduces the time consumption and dependency over the nodes.

4. Performance Evaluation

4.1. A. Simulation Model and Parameters

We use NS2 to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2Mbps. We use the Distributed Coordination Function (DCF) of IEEE802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, mobile nodes move in a (1000m× 1000m) square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250m. In our simulation, the speed is varied from 10m/s to 50m/s and the number of nodes is varied from 20 to 100. We fix 10% of the total nodes as attackers. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 1.

Table 1.Simulation settings.

No. of Nodes	20,40,60,80 and 100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Attackers	10% of the nodes
Speed	10,20,30,40,50m/s
Pause time	5

4.2. Performance Metrics

We evaluate mainly the performance according to the following metrics.

- *Control Overhead*: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.
- *Average End-to-End Delay*: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.
- *Average Packet Delivery Ratio*: It is the ratio of the number .of packets received successfully and the total number of packets transmitted

The simulation results are presented in the next section. We compare our EDCA protocol with our previous TCLS protocol [11] in presence of malicious node environment.

4.3. Results

a. *Based on Nodes*: In our first experiment, we vary the number of nodes as 20,40,60,80 and 100 by keeping the node speed as 10m/s.

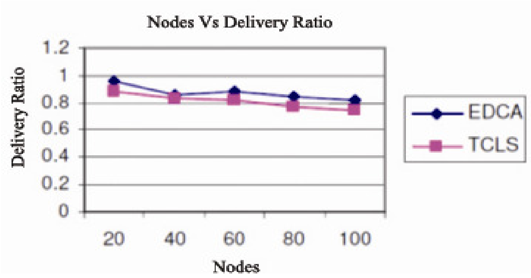

Figure 1. Nodes vs delivery ratio.

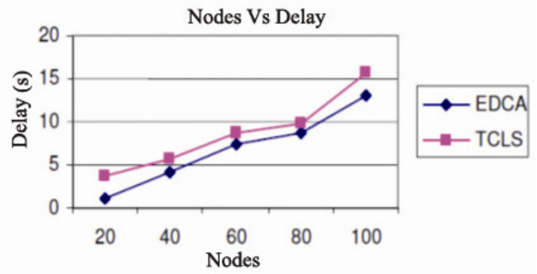

Figure 2. Nodes vs delay.

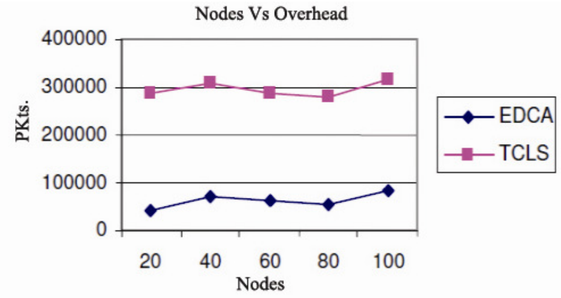

Figure 3. Nodes vs overhead.

Figure 1 shows the results of average packet delivery ratio for varying the nodes from 20 to 100. Clearly our EDCA scheme achieves more delivery ratio than the TCLS scheme since it has both reliability and security features.

Figure 2 shows the results of average end-to-end delay for varying the nodes from 20 to 100. From the results, we can see that EDCA scheme has slightly lower delay than the TCLS scheme because of authentication routines.

Figure 3 shows the results of routing overhead for the varying nodes. From the results, we can see that EDCA scheme has less routing overhead than the TCLS scheme since it does not involve route re-discovery routines.

b. *Based on Speed*: In our second experiment, we vary the node speed as 10,20,30,40 and 50, with 100 nodes.

Figure 4 shows the results of average packet delivery ratio for the speed 10, 20…50 for the 100 nodes scenario. Clearly our EDCA scheme achieves more delivery ratio than the TCLS scheme since it has both reliability and security features.

Figure 5 shows the results of average end-to-end delay for the speed 10, 20….50. From the results, we can see that EDCA scheme has slightly lower delay than the TCLS scheme because of authentication routines.

Figure 6 shows the results of routing overhead for the speed 10, 20….50. From the results, we can see that EDCA scheme has less routing overhead than the TCLS scheme.

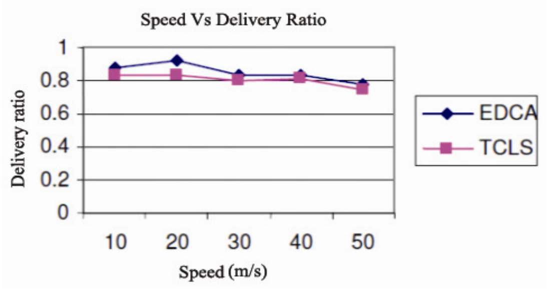

Figure 4. Speed vs delivery ratio.

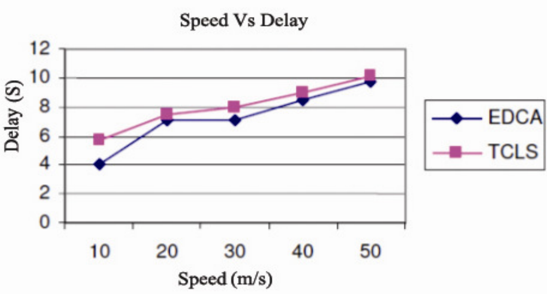

Figure 5. Speed vs delay.

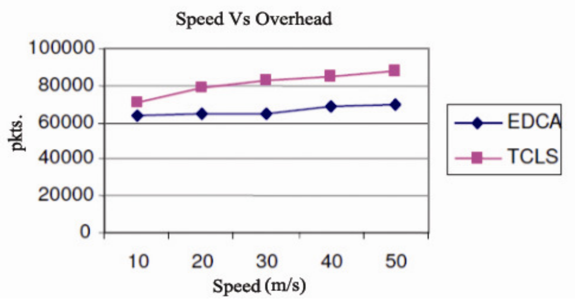

Figure 6. Speed vs overhead.

5. Conclusions

In this paper, we have extended our previous work on trust counters by using a certificate authority to provide integrity of our network along with resisting attacks from outside. Our work is a three phase scheme consisting of; RCF of packet monitoring, Certification revival and Certification revocation. Using our previous work we monitor the routing and packet forwarding behaviors of the nodes in each hop. We use Shamir's secret sharing model with redundancy for Certification revival and revocation. When we use redundancy the challenges of node mobility reduces as it states that the total number of nodes requisite to recreate the CA key can be less than *(k-1)*. This increases the integrity of the network and provides the network nodes to be more mobile. Certification revocation is done using the trust values of the nodes. By simulation results, we have shown that the proposed scheme achieves more packet delivery ratio while attaining less delay and overhead, compared with the previous existing scheme.

References

[1] Akbani R., Korkmaz T., and Raju G., "HEAP: A Packet Authentication Scheme for Mobile Ad-hoc Networks," *Ad-hoc Networks*, vol. 6, no. 7, pp. 1134-1150, 2008.

[2] Amitabh M., *Security and Quality of Service in Ad-hoc Wireless Networks*, Cambridge University Press, UK, 2008.

[3] Bing W., Jianmin C., Jie W., and Mihaela C., "A Survey on Attacks and Countermeasures in Mobile Ad-hoc Networks," *in Proceedings of Wireless Network Security, Signals and Communication Technology*, pp. 103-135, 2007.

[4] Deepti J., Kamesh N., and Ravi P., "Secure, Redundant, and Fully Distributed Key Management Scheme for Mobile Ad-hoc Networks: An Analysis," *Journal on Wireless Communications and Network*, vol. 2005, no. 4, pp. 579-589, 2005.

[5] Farooq A. and Petros M., *Security for Wireless Ad-hoc Network*, John Willy and Sons, 2007.

[6] Komninos N., Vergados D., and Douligeris C., "Detecting Unauthorized and Compromised nodes in Mobile Ad-hoc Networks," *Ad-hoc Networks*, vol. 5, no. 3, pp. 289-298, 2007.

[7] Mark E., Timothy E., and Cynthia E., "An Ontological Approach to Secure MANET Management," *in Proceedings of the 3rd International Conference on Availability, Reliability and Security*, Barcelona, pp. 787-794, 2008.

[8] Mohammed A. and Zuriati A., "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment," *European Journal of Scientific Research*, vol. 32, no. 3, pp. 430-443, 2009.

[9] Nitesh S., Tsudik G., and Jeong H., "Threshold Cryptography in P2P and MANETs: The Case of Access Control," *Elsevier Computer Networks*, vol. 51, no. 12, pp. 3632-3649, 2007.

[10] Prasant M. and Srikanth K., *Ad-hoc Networks: Technologies and Protocols*, Springer, 2005.

[11] Rajaram A. and Palaniswami S., "A Trust-Based Cross-Layer Security Protocol for Mobile Ad-hoc Networks," *International Journal of Computer Science and Information Security*, vol. 6, no. 1, pp. 165-172, 2009.

[12] Shafiullah K., Kok-Keong L., and Zia D., "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 435-440, 2010.

[13] Sreedhar C., Madhusudhana V., and Kasiviswanath N., "A Survey on Security Issues in Wireless Ad-hoc Network Routing Protocols," *International Journal on Computer Science and Engineering*, vol. 2, no. 2, pp. 224-232, 2010.

[14] Stamatios V., *Security of Information and Communication Networks*, Wiley-IEEE Publications, USA, 2009.

[15] Vaidya B., Sang-Soo Y., and Dong-You C., "Robust and Secure Routing Scheme for Wireless Multihop Network," *in Proceedings of the Personal and Ubiquitous Computing*, UK, vol. 13, pp. 457-469, 2009.

[16] Wenbo H., Ying H., Ravishankar S., Klara N., and Whay C., "SMOCK: A Scalable Method of Cryptographic Key Management for Mission-Critical Wireless Ad-hoc Networks," *IEEE Transactions on information forensic and security*, vol. 4, no. 1, pp. 140-150, 2009.

[17] Wikipidia, "Shamir's Secret Sharing," available at: http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing, last visited 2011.

[18] Yan Z., Jun Z., and Honglin H., *Security in Wireless Mesh Networks*, Auerbach Publications, 2009.

Rajaram Ayyasamy received the BE degree in electronics and communication engineering from the Govt., college of Technology, Coimbatore, Anna University, Chennai, India, in 2006, the ME degree in electronics and communication engineering (Applied Electronics) from the Govt., college of Technology, Anna University, Chennai, India, in 2008 and he received the Ph.D. degree in electronics and communication engineering from the Anna University of Technology, Coimbatore, India in March 2011. He is currently working as a Associate Professor, ECE Department in Karpagam College of Engineering, Coimbatore, India. His research interests include mobile adhoc networks, wireless communication networks (WiFi, WiMax HighSlot GSM), novel VLSI NOC Design approaches to address issues such as low-power, cross-talk, hardware acceleration, Design issues includes OFDM MIMO and noise Suppression in MAI Systems, ASIC design, Control systems, Fuzzy logic and Networks, AI, Sensor Networks.

Palaniswami Subramani received the B.E. degree in electrical and electronics engineering from the Govt., college of Technology, Coimbatore, University of Madras, Madras, India, in 1981, the M.E. degree in electronics and communication engineering (Applied Electronics) from the Govt., college of Technology, Bharathiar University, Coimbatore, India, in 1986 and the Ph.D. degree in electrical engineering from the PSG Technology, Bharathiar University, Coimbatore, India, in 2003. He is currently the principal of Thanthai Periyar Government Institute of Technology, Vellore, India. His research interests include Control systems, Communication and Networks, Fuzzy logic and Networks, AI, Sensor Networks. . He has about 25 years of teaching experience, since 1982. He has served as lecturer, Associate Professor, Professor, Registrar and the life Member of ISTE, India.