Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.693 – 700

RESEARCH ARTICLE

CLUSTER ENHANCED SECURE AUTHENTICATION SCHEME FOR DATA INTEGRITY IN MANET

A. Praveena (PG Scholar), **Dr. L.M. Nithya** (HOD)
Department Of Information Technology,
SNS College of Technology, Coimbatore-35
Praveena035@gmail.com

Abstract—Mobile ad hoc networks (MANETs) consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies. Due to high mobility of nodes, there exist frequent link breakages which lead to frequent path failures and route discoveries. In a route discovery, both cluster and broadcasting scheme is deployed, where a mobile node blindly rebroadcasts the first received route request packets unless it has a route to the destination, and it causes the broadcast storm problem. In cluster based multipath routing scheme is proposed for reducing routing overhead and energy consumption in MANETs. Multipath routing with cross layer framework is proposed to effectively exploit the load balancing and also to improve the network lifetime, accurate additional coverage ratio of cluster is determine the sensing cluster member coverage knowledge. Packet integrity is determined to provide the hop to hop authentication. By combining the cluster and cross layer frame work, a reasonable node lifetime is set to improve communication coverage. This scheme combines the advantages of the new enhanced RSA encryption/decryption scheme and energy consumption model which can significantly decrease the number of retransmissions so as to reduce the routing overhead, energy consumption, vulnerability of attackers and can also improve the network lifetime.

Keywords—Mobile ad hoc networks (MANETs), Energy Consumption, Security, Data Integrity, and Load Balancing

I. Introduction

Mobile Ad-hoc Network (MANET) is a self-configuring infra-structure less network of mobile devices connected by wireless links. The node that has the mobility is called the mobile node, mobility means moving around the world. Each device in a MANET is free to move alone in any direction and will change its links to other devices frequently. Each must forward traffic separate to its own use and a router. The primary challenge in building a MANET is providing each device to continuously maintain the information required to properly route traffic. Such networks may be operate by them or may be connected to the larger Internet. MANETs are one kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. Certificate revocation is an important task of enlisting and removing the certificates of nodes who have been detected to launch attacks on the region. In other words, if a node is undermined or misbehaved and it should be removed from the network and cut off from all its activity immediately.

Certificate management is a widely used mechanism which serves as a mean of conveying trust in a public key infrastructure to secure applications and network services. Complete security solutions for certificate management should encompass three components: prevention, detection and revocation. Certification is prerequisite to secure network communication. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer and can be used to verify that a public key belongs to an individual and to prevent tampering, forging in mobile ad hoc networks. Consequently, a mobile ad hoc network is vulnerable to many kinds of malicious attacks and it is difficult to ensure secure communications. Malicious nodes directly threaten the durableness of the network as well as the availability of nodes. Protecting legal nodes from malicious attacks must be considered in ad hoc networks. This is achievable through the use of a key management scheme which conveying trust in a public key infrastructure. These certificates are proved by the Certificate Authority (CA) of the network, which is a trusted third party and responsible for issuing and revoking certificates.

The mechanism performed by the CA plays an important role in enhancing network security. It digitally signs a valid certificate for each node to ensure that nodes can communicate with each other in the network. In such networks, a certificate revocation scheme which invalidates attacker’s certificates is essential in keeping the network secured. An attacker’s certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. However, it is difficult for the CA to determine if an accusation is trustable because malicious nodes can potentially make false accusations. A malicious node will try to remove legitimate nodes from the network by falsely accusing them as attackers. Therefore, the issues of false accusation must be taken into account in designing certificate revocation mechanisms.

II. Related Work

Wei Liu describes, certificate revocation is an important integral component to secure network communications. The issue of certificate revocation to isolate attackers from further participating in network activities. For quick and accurate certificate revocation, propose the cluster-based certificate revocation with vindication capability scheme [1].In particular, to improve the reliability of the scheme, recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks.

K.Park describes, certification systems play an important role in maintaining network security because attackers can freely move and repeatedly launch attacks against different nodes. A simple way to identify attackers is based on to collect information on attackers from nodes in the network [2]. To reduce the damage from attacks, attackers must be immediately removed from the network after detection of the first attack. This can be achieved by using a certification system; nodes cannot communicate with each other without a valid certification. In other words, any attacker cannot exist in the network once its malicious behavior has been detected by others and its certification has been revoked accordingly by the system.

G.Arboit says that, the issue of certificate revocation in mobile ad hoc networks where there is no on-line access to trusted authorities. In purely ad hoc networks, there is typically no access to centralized repositories or trusted authorities; therefore the conventional method of certificate revocation is not applicable [3].A decentralized certificate revocation scheme that allows the nodes within a MANET to revoke the certificates of malicious entities.

Mike Burmester describes, communications is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view. This security model is that it promises security guarantee under concurrent executions, a crucial practical implication for this type of distributed computation [4].A new security framework tailored for on-demand route discovery protocols in MANET. This represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks. The attacks that are intrinsic to the wireless broadcast medium in a neighborhood. Three basic phases in routing: Route discovery in which one or more routes that link a source to a target. Route maintenance in which broken links of established routes are fixed. Packet forwarding in which communication is achieved via established routes.

III. Problem Definition

A.Exisisting System

In existing, Certificate revocation is an important integral component to secure network communications. The issues of certificate revocation to isolate attackers from further participating in network access. For quick and accurate certificate revocation, propose cluster based certificate revocation with vindication capability scheme. Certificate revocation mechanisms play an important role in securing a network. When the certificates of malicious nodes are revoked and it is denied from all activities and isolated from the network.

The main challenges for certificate revocation are to revoke the certificates of malicious nodes promptly and accurately. Two neighboring nodes receive their certificates from each other and also exchange certificate information about other nodes that they know. Nodes sharing that the same certificate information is regarded as belonging to the same networks. In these networks, the certificates of a suspected node can be revoked when the number of accusations against the node exceeds a certain threshold.

B. Cluster-Based Certificate Revocation Scheme

A centralized Certificate Authority (CA) manages certificates for all the nodes in the network cluster construction is decentralized and performed autonomously. Nodes cooperate to form clusters and each cluster consists of a Cluster Head long with several Cluster Members that are located within the communication range of their CH. Each CM belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap a node within the communication range of a CH is not necessary part of its cluster. The aim of using clusters is to enable CHs to detect false accusations. Requests for the CA to recover the certificates of falsely accused nodes can only be made from CHs.

A CH will send a Certificate Recovery Packet to the CA to recover an accused node only in the case where it is a CM in its cluster. This is based on the fact that most types of attacks, such as flooding attack, black hole attack, wormhole attack and Sybil attack, can be detected by any node within the communication range of the attacker. In other words, a cluster head will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not. A centralized Certificate Authority (CA) manages certificates for all the nodes in the network cluster construction is decentralized and performed autonomously.

Nodes cooperate to form clusters and each cluster consists of a Cluster Head long with several Cluster Members that are located within the communication range of their CH. Each CM belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap a node within the communication range of a CH is not necessary part of its cluster. The aim of using clusters is to enable CHs to detect false accusations. Requests for the CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet to the CA to recover an accused node only in the case where it is a CM in its cluster. This is based on the fact that most types of attacks, such as flooding attack, black hole attack, wormhole attack and Sybil attack, can be detected by any node within the communication range of the attacker. In other words, a cluster head will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not.

C. Proposed System

Cluster based certificate revocation with vindication capability scheme is more effective and efficient in revoking certificates of malicious attacker nodes reducing revocation time and improving the accuracy and reliability of certificate revocation. The significant advantages of the voting-based mechanism are the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision processes to satisfy the condition of certificate revocation is slow.

Also, it incurs heavy communications overhead to exchange the accusation information for each other. The non-voting-based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. The accuracy of determining an accused node as a malicious attacker and the reliability of certificate revocation will be degraded as compared with the voting-based method.

To provide both data integrity and authentication and to secure multipath route to improve network lifetime. Ensure certificate revocation for identifying active and passive attackers. To enhance cluster route with maximum threshold value for providing more security and enable cryptography based encryption and decryption scheme. Secure multipath route can be implemented. Cluster threshold point will be maintained. More network and node authentication can be maintained. Anonymous route selection will be identified quickly. Applicable to all public services and disaster applications.

IV. Multipath Routing

The Multipath provides high throughput and more network lifetime. Multipath is used in conjunction several authentication techniques. Here hop to hop authentication is used to find the efficient path to improve network lifetime. This authentication is also known as multipath authentication. Nodes are organized in a cluster group. Each cluster group communicates via multipath routing to maintain their effective communication and less communication overhead.

In Cluser1, Cluster Head 1 chooses the multipath to Cluster Head 2. If the cluster nodes want to send a packet to another cluster in different region, it should get authentication from both cluster head. If any node failure occurs, the route control message is forwarded to both cluster regions. The failure means like node failure, path failure, link failure, etc.

To avoid this, the disjoint paths are chosen. Information is sent over multiple strictly disjoint paths. If different versions of information are received, the destination chooses the highest priority. So the remaining paths may be considered as dishonest, since it is delivered a seemingly incorrect message.

A. Assumptions made to construct proposed multipath routing:

1. More number of cluster nodes need to spend energy on routing.
2. If Multiple disjoints paths are used, it require a minimum degree of connectivity.
3. Loosely connected nodes cannot be used and it cannot get profit from multipath routing.
4. Determining and maintaining sets of disjoint paths between two communication endpoints are difficult in multipath, compared to a single path.
5. If the message is delivered in to the different parts of the network, the multipath routing will get effect in to network partitioning.
6. Only chosen packets with less capacity can be sent via routing.
7. More stability of the path is used in multipath routing.

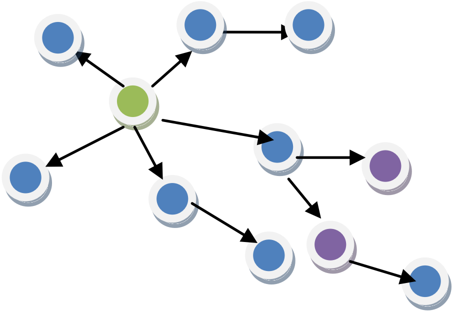

Fig.1. Mulitpath Routing Discovery Procedure

In Fig.1, the multipath route discovery is illustrated to ensure more load balancing and network lifetime. Source node sends its packet to destination via multipath. If any path failure occurs , alternate shortest path will be chosen based on the stability of it. The main aim is to make network connectivity more by making the packet arrival time very less.

In multipath routing, it is assumed that source node S has three paths to destination D. If any path failure occurs, the source node will choose another path to reach packet at the destination. A message can be sent on alternating paths, or on multiple paths in parallel. Both reduce the impact of isolated failures.

V. Cluster Head Election

In the proposed hybrid cluster enhanced secure multicast routing scheme, cluster heads are responsible for cluster formation and maintain the network security. If cluster head discloses confidential information, it will imperil the security of the system. Including this, due to dynamic nature of the mobile nodes, their organization and dissociation to and from clusters trouble network stability and thus reconfiguration of cluster heads is necessary.

Step1. Determine the level of convicted accusation. Each cluster member stores the accusation of insecure nodes in its Cluster member Certificate Revocation List (CRL), and then forwards the information of accusations to neighbors who store it in their CRL with a "suspect" accusation. The level of convicted accusation is S_u. Once the node gathers P accusations of a certain node, the "suspect" becomes "convicted." The P is the value in an (n, k) threshold cryptography scheme. The greater S_u indicates more insecure.

Step2. Estimate the convicted accusation S_u . If the S_u of the node u equals P, then node u is a malicious node. Consequently, the node u is eliminated from the election. Otherwise, the following procedures are to be implemented.

Step3. Value the reliable degree of node *u*. This study introduces the function of trust valuation in disclosed networks to evaluate direct trust relationships between two nodes. The combined value is calculated as

$$U_{comb} = 1 - \prod_{k=1}^{l} \sqrt[n_l]{\prod_{d=1}^{n_k} (1 - U_{k,d})} \qquad (1)$$

Where $U_{k,d} \neq 0$ where, $V_{k\ d}$ denotes the value of the derivation of multiple direct trust relationships between two nodes;

V_{comb} represents the combined value of direct trust relationships in which *k* trusts *d*. In this scheme, after a period of operations, since each cluster member has the accused record of other nodes in its own CRL, the accused record indicates that the trust value between two cluster members and is shared among all members via RREQ messages, enabling the direct or recommended trust value to be derived.

Step4. Find the cluster neighbors of each member *u* which define its degree d_u as,

$$d_u = | M(u) | = \sum_{u' \in U, u' \neq u} \{ dist(u, u') < ty_{range} \} \qquad (2)$$

Step5. Compute the degree difference $\Delta u = |d_u - \delta|$, for every node *u*. To ensure efficient Medium Access Control (MAC) functioning, each cluster head can support an optimum of δ, a pre-defined threshold of cluster members. This value exists to ensure that a cluster head does not become overloaded and the system efficiency is maintained at the expected level.

Step6. For every cluster member *u*, compute the sum of distances *Du* with all neighbors, as

$$D_u = \sum_{u' \in N(u)} \{ dist(u, u') \} \qquad (3)$$

Step 7: Determine the operation average speed for every node until the current time is τ . Cluster members are assumed to have a Global Positioning System (GPS) since the GPS is primarily used to determine the geographical location of mobile nodes.

Step8. Compute the battery power consumption P_u, which is assumed to be more for a cluster head than an ordinary node.

Step9. Calculate the combined weight W_u for each cluster member *u* in cluster

Step10. Choose the node with the smallest W_u as the cluster head. All the neighbors of the chosen cluster head are no longer permitted to participate in the election procedure.

Step11. In the other clusters, repeat steps 1–10 to elect cluster heads for the remaining nodes not yet selected as a cluster head or assigned to a cluster.

Step12. Choose the cluster head with the smallest W_u as the root cluster head R_{ch}.

VI. Secure Authentication Scheme

In this phase, both encryption and decryption schemes are implemented. Here three types of iterations are used while converting plaintext to ciphertext. In first iteration, plaintext is converted into ASCII value. In second, ASCII is converted into BCD value. In third, BCD is converted in to Hexadecimal value.

The following cryptographic basics are used in PSEC:

1. KDF is a key derivation function that is constructed from a hash function.

2. ENC is the encryption function for a symmetric-key encryption scheme such as the AES, and DEC is the decryption function.

3. MAC is a message authentication code algorithm such as HMAC.

Encryption phase

B can encrypt a message m for A, which A can decrypts.

Encryption, B should do the following:

(a) Obtain A’s authentic public key n.

(b) Represent the message m as a string m = m1 m2 mt of length t, where each mi is a binary string of length h.

(c) Select as a seed x0, a random quadratic residue modulo n. (This can be done by selecting a random integer r ∈ Zn and setting x0←r2 mod n.)

(d) For i from 1 to t do the following:

i. Compute xi = x2 i−1 mod n.

ii. Let pi be the h least significant bits of xi.

iii. Compute ci = pi XOR mi.

(e) Compute xt+1 = x2t mod n.

(f) Send the ciphertext c = (c1, c2, . . . , ct, xt+1) to A.

Decryption phase

Decryption. To recover plaintext m from c, A should be do the following:

(a) Compute d1 = ((p + 1)/4)t+1 mod (p − 1).

(b) Compute d2 = ((q + 1)/4)t+1 mod (q − 1).

(c) Compute u = xd1 t+1 mod p.

(d) Compute v = xd2 t+1 mod q.

(e) Compute x0 = vap + ubq mod n.

(f) For i from 1 to t do the following:

i. Compute xi = x2 i−1 mod n.

ii. Let pi be the h least significant bits of xi.

iii. Compute mi = pi XOR ci.

Mathematical Proof:

Key Generation:

Entity A selects the primes p = 499, q = 547, each congruent to 3 modulo 4, and computes n = pq = 272953.

Using the extended Euclidean algorithm, A computes the integers a = −57, b = 52 satisfying ap+bq = 1. A’s public key is n = 272953, while A’s private key is (p, q, a, b).

Encryption. The parameters k and h have the values 18 and 4, respectively. B represents the message m as a string $m_1m_2m_3m_4m_5$ (t = 5) where m_1 = 1001, m_2 = 1100, m_3 = 0001, m_4 = 0000, m_5 = 1100.

B then selects a random quadratic residue x_0 = 159201 (= 3992 mod n), and computes c.

Decryption:

i	**$x_i = x^2_{i-1}$ mod n**	**p_i**	**$c_i = p_i \ m_i$**
1	180539	1011	0010
2	193932	1100	0000
3	245613	1101	1100
4	130286	1110	1110
5	40632	1000	0100

- c = (0010, 0000, 1100, 1110, 0100, 139680)
- Decryption. To decrypt c, A computes
- d1 = $((p + 1)/4)^6$ mod (p − 1) = 463
- d2 = $((q + 1)/4)^6$ mod (q − 1) = 337
- u = x_6^{463} mod p = 20
- v = x_6^{337} 6 mod q = 24
- x_0 = vap + ubq mod n = 159201.
- Finally, A uses x_0 to construct the x_i and p_i just as B did for encryption, and recovers the
- plaintext m_i by XORing the p_i with the ciphertext blocks c_i.

VII. Conclusion

In this paper, addressed a major issue to ensure secure communications for MANETs namely certificate revocation of attacker nodes. In difference to existing algorithms, we propose a CCRVC scheme combined with the merits of both voting-based mechanism and non-voting-based mechanism, to cancel malicious certificate and solve the problem of false accusation. The scheme can cancel an accused node based on a single nodes accusation and reduce cancellation time as compared to the voting-based mechanism. In addition, have adopted the cluster-based model to replace falsely accused nodes by the cluster head thus making better the accuracy as compared to the non-voting-based mechanism.

Particularly, have proposed a new motive method to release and replace the legitimate nodes and to refine the number of available normal nodes in the network. Have the sufficient nodes to ensure the efficiency of quick cancellation. The immense results have disclosed that in difference with the existing methods our proposed cluster-based certificate revocation with vindication capability scheme is more effective and efficient in canceling certificates of malicious attacker nodes, reducing cancellation time, improving the accuracy and validity of certificate revocation.

References

[1] Wei Liu, Hiroki, Nishiyama, Nirwan Ansari,“Cluster-BasedCertificate Revocation with Vindication Capability for Mobile Ad Networks,” IEEE Transactions on Parallel and Distributed Systems, vol.24, No.2, Feb 2013.

[2] K. Park, H. Nishiyama, N. Ansari, and N. Kato, “CertificateRevocation to Cope with False Accusations in Mobile Ad HocNetworks,” Proc. IEEE 71st Vehicular Technology Conf. (VTC ’10),May 16-19, 2010.

[3] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, “A Localized CertificateRevocation Scheme for Mobile Ad Hoc Networks,” Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[4] Mike Burmester,“On the Security of Route Discovery in MANETs”,IEEE Transactions on Mobile Computing, Vol. 8, No. 9, September 2009.

[5] Kalpana Sharma, M.K. Ghose, International Journal of Security and Its Applications, “Cross Layer Security Framework for Wireless Sensor Networks,” Vol. 5,No. 1, January, 2011.

[6] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks,” IEEENetwork Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 2006.

[7] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On theDistribution and Revocation of Cryptographic Keys in SensorNetworks," IEEE Trans. Dependable and Secure Computing, vol. 2,no. 3, pp. 233-247, July 2005.

[8] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[9] J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks,"IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489,Dec. 2007.

[10] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N.Kato, "A Survey of Routing Attacks in MANET," IEEE WirelessComm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.