International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Authentication in Mobile Ad Hoc Network for Secure Communication

Tejashree Kokate[1], R.B.Joshi[2]

[1]Marathwada Mitramadal college of Engineering, Savitribai Phule Pune University Pune, Maharashtra, India

[2]Ph.D. scholar JJT University,Rajasthan, Asso. Professor,Computer Engineering Dept.,ICEM Pune, SavitribaiPhule PuneUniversity Pune, MMCOE, Pune, India

Abstract: ***For wireless applications the main concern is security. The provisions done for securing the application become bottleneck for widely deployed wireless applications as they affect efficiency. Wireless channels need to be secure. Also it becomes bottleneck because wireless bandwidth is a constrained resource. To achieve security according to the available resource without affecting efficiency is desirable. In particular, mobile adhoc networks (MANETs) based on cooperative communication present significant challenges to security issues, as well as issues of network performance and management. In this paper, we focus on authentication and topology control for mobile ad hoc network. TESLA scheme is proposed to improve the throughput. The scheme proposed works well where no prior information about network is available i.e., for dynamic environment. Results show that our scheme has a capacity to substantially improve throughput in MANETs.***

Keywords: mobile ad hoc network authentication, markle tree authentication, cooperative communication, TESLA scheme, message authentication for broadcasting, cooperative communication, dynamic network authentication.

1. Introduction

Authentication of the users of application stops unwanted access to the system. As multiple-hop communications are used in mobile ad hoc networks with Cooperative communication schemes (CC-MANETs), not only end-to-end (e2e) but also hop-by-hop (HBH) authentication, message integrity, secure message transfer are required to protect the network from intruders and forging of packets by malicious nodes. As wireless technology adds to ease and accuracy for dynamic environment it has become most popular for application development but at the same time the main concern for widely deployed wireless applications is of secure data transfer [1]. Mainly two points need to taken care off: First is as wireless is open shared access platform it is vulnerable to intruders. Second, the wireless resources have many constrains e.g. bandwidth. Security is achieved at the cost of performance degradation. Security with available resources without much performance degradation in the network is need of the hour. Mobile ad hoc network applications should consider topology control and authentication simultaneously. As nodes are dynamic authentication process should have track of the node with the help of topology control. Topology control using TESLA uses basic idea of considering the network static for a moment. Topology control is the key factor which optimizes network performance in a network-wide perspective. Self-organization of nodes, neighbor discovery and topology organization, topology control are important tasks in MANETs. Changing position of nodes over time, managing transceiver parameters for data transfer is time critical. Topology control is referred to as selecting a set of neighbors to establish logical links and dynamically adjust the transceiver parameters [11]. Existing topology control schemes work on adjusting the physical (PHY)-layer or medium-access control (MAC)-layer parameters, such as transmission power and interference, to improve the overall network performance. In this paper mainly we concentrate on the Authentication scheme. For this we use Markel Tree for the Public key private key distribution. Here we use the Hash chaining concept to make the authentication strong. Same way we use TESLA i.e. Timed, Efficient, Streaming, Loss-tolerant, Authentication protocol. In this, time is divided equally and key is generated with reference to the current time.

Rest of the paper is organized as follows: Section II provides Security requirements of MANET, Section III describes the Authentication protocol based on Hash chain & Markel Tree, Section IV proposed work, Section V Implementation Section VI Result Analysis and Conclusion.

2. Security Requirements Of Manets

The must have requirements for mobile ad hoc network securities are as follows:

Authentication of message and integrity: it protects from alteration of data to be transmitted and ensures the receiver that message is from right source and is not changed in between.

Message Non-Repudiation: it makes sender responsible for the messages he sent i.e., sender of a message cannot deny having sent a message.

Entity Authentication: In this receiver is ensured that the sender generated a message and has evidence of the liveness of the sender. In other words, ascertain that a received unmodified message was generated within an interval. This is achieved by time stamping the messages in many schemes.

2.1 Literature Survey

Noteworthy existing work on MANET authentication is as follows:

1) Multi-factor authentication: This system provides multiple authentications to verify true nature of a transaction. This multi-factor authentication scheme extends the cryptographic link, binding an entity to a physical node device. It uses two different authentication factors; certified keys and certified node characteristics. But the major drawback is that, the underlying networking environment on which they are applicable have been left unspecified. But here lack of specifications about networking environment which are used by authenticating protocol is misled. [2]
2) Authentication and dynamic key management protocol
3) based on certified tokens for MANETs: In this no centralized authority is used for storing the key in active stage. It uses RSA algorithm and Elliptic curve cryptography together for authentication. This combination also decides key agreement protocol. This protocol serves the purpose of making applications lightweight without using much of storage space. But everything i.e., key agreement, key designing and exchange of key is done at run time. This gives rise to high computational and communicational overhead. Besides such scheme provides secure data exchange environment. [3]
4) Certficateless authentication: It uses threshold signature which is employed with combination of RSA algorithm and secret sharing Shamir's scheme. Threshold cryptography is employed for distribution of private key among user nodes.
5) Establishing stable certificate chains for authentication: This scheme is developed to face the odds caused by unstable topology and link failure in MANETS. In this route selection algorithm has link expiry time parameter. Link expiry time helps in selecting proper links and avoids link failure.

Sr No	System	Drawbacks
1	Multi-factor authentication[2]	Lack of specifications about the networking environments
2	Distributed Authentication Scheme and Trusted Computing[3]	The secure and practical authentication problem in it becomes outstanding
3	Authentication and dynamic key management protocol based on certified tokens[4]	It contains no pre-key distributions and key storage for making protected data transmission
4	Key distribution with entity authentication for efficient, scalable communication[5]	No central authorization entity is assumed at all times

Figure 1: Table of Different Techniques and drawbacks

The overview of existing systems and their drawbacks are listed in table. Our system aims to remove the drawbacks seen in the existing system by using markle tree for designing the key which will be different for each node.

3. Authentication Protocol

A combination of Merkel trees and interactive signatures is used in Hash chain authentication. Any cryptographic hash function H(x) when successively applied by hashing random seed variable x becomes a hash chain. It is applied in opposite sequence since hi can be revealed only after hi minus 1.

The owner initially provides the last element of hash chain to the verifier. Later by hashing hi minus 1, the verifier is able to establish authenticity of the owner with hi minus 1. An efficient key management which minimizes the size and amount of public keys is necessary to for feasibility of One-Time Signature Schemes. A Merkel Tree is a binary tree with hashes of data messages as its leaves and nodes being the concatenation of their respective children. The root, calculated by the leaves and nodes, then serves as pre-signature information. While routing of message packet from the source, each node of the Merkel tree implantation provides a new hash value; hence making data more secure. The route node is the public key of this scheme.

When the message packet is to be routed from source, for each node markle tree implementation provides new hash value; this makes the data more secure. For inner nodes of the tree the hash value is concatenation of children hash values. e.g. A[0,1]=A(0,0)|| A(0,1) The route node is the public key of markle signature scheme.(ref fig 2)

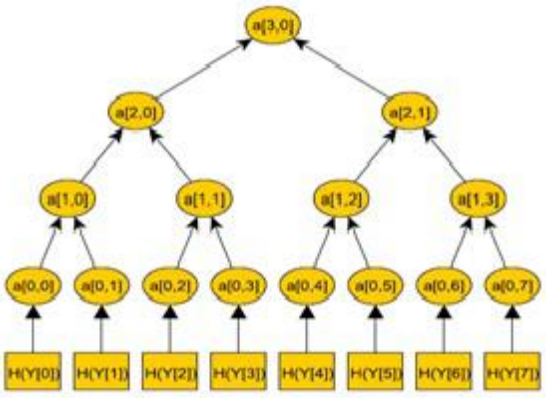

Figure 2: Markle tree with 8 leaf nodes

4. Proposed Work

In multicasting system the authentication with low overhead, secure method of time synchronization and time series event correlation is presented. The method described in this paper integrates tightly with the secure routing, key exchange, and management with TESLA-based network gives secure message transfer. To optimize network performance in a network-wide perspective the major activities involved in self organization are neighbor discovery and topology organization, where topologies are changing over time as nodes are moving.

We assume the network as static network at a particular time of instance and apply the algorithm. To discover the neighbor nodes, we flood a dummy token to all nodes and calculate the shorted acknowledge time. This is applied to all the nodes and find out the topology for a particular time of instance (where we are considering the network is static) with the help of Dijkstra shortest path algorithm. The message is forwarded to the nearest node using the RSA encryption algorithm to provide strong authentication security. For the key distribution (exchange)the Diffie Hellman algorithm to exchange the public key. The system is designed for authentication and topology control using combination of algorithms. System aims to work in three phases:

Phase 1: In this nodes in the network which are moving can send the data on one to one basis i.e., one node can send information to other node in the network.

Phase 2: In this multicasting of network nodes is to be achieved i.e., One node should be able to send message packets to group of nodes in the network.

Phase 3: It attempts to make broadcasting of data possible for nodes in the network. In the proposed system, time is divided into intervals. Every interval has a key for signing also key for public disclosure during that interval. Both keys are part of the same one-way chain, in a sequence signing key and then disclosed key.

Signing key can't be calculated from the disclosed key, but disclosed key can be calculated from signing key by computing the hash of the signing key a determinate number of times.

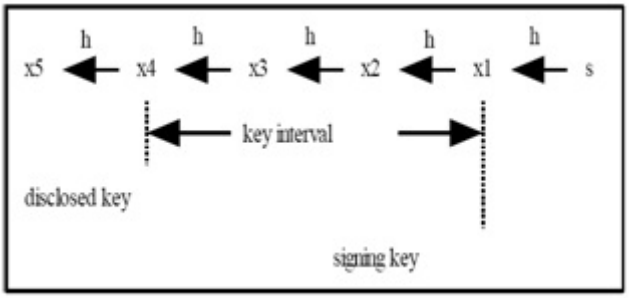

Figure 3: Position of disclosed key and signing key

As shown in Figure 3, the disclosed key occurs a set distance from the signing key in the one-way chain , this distance is called the key interval. When time has passed and the server is in the next time interval, the messages in that interval would be disclosing key x3 and signed with keys.

As the client receives messages, it queues them until an Interval has passed that is equal to the key interval. Messages. That is sent during this interval will disclose a key that was used to sign a subset of the messages in the queue. We can prove that this message has been sent from the same entity that sent the earlier messages by showing that the disclosed keys are all part of the same chain.

5) Mathematical Model for system: Let A be the set that describes the set for System,

Let A be the set that describes the set for System = {N,T,P,X,T}

N = Number of nodes, such that $\{n_1,...,n_N\}$ is set of mobile ad hoc network nodes.

Ns = Sender node that wishes to send the data.

T = { t_1, t_2,...,t_K } set of time intervals selected by the Sender n_S

f(x) = RSA(x) used for the generation of keys used for the encryption.

P = {f(x)^1,f(x)^2,f(x)^3,...,f(x)K} be the value used for the encryption by considering x = {1,2,3,...,K}with respect to the time T = { t_1, t_2,...,t_K }

Signer key for encryption is markle tree root calculated at run time.(depending on the tree and it's nodes)

Let B is the set that describe set for encryption and decryption,

B = {C_i , n_i}

C_i = enc(f(x)$_i$, msg) be the cipher text after encrypting message msg using key f(x)$_I$ such that i={1,2,3,...,K}.

Let n (i) be the node which has authenticated sender node nS. Sender node nS obtains the nodes to be traversed to reach destination node with dikstra's algorithm. It gets message from user. Sender n_S synchronizes its time clock with all nodes N

4. n_S then generates set of f(x)n$_i$ = {f(x)$_1$,f(x)$_2$,...,f(x)$_K$}for every node n$_i$

5. Assume t_C *is* current time and r is value specific to network conditions node n_S then calculates time slots $t_{(C4r)}$ - t_C

6.source node then assigns set { f(x)$_1$,f(x)$_2$,...,f(x)$_K$} of every node to all time slots onwards t_C up to t_{c+r}

7. Node nS then takes the message m and splits into p blocks such as,

$$m = \sum_{i=1}^{p} m_p$$

8. At every time interval source node take message mi and encrypts it as Ci =encrypt(f(xi), mi)

For every node and n_j sends it node n_j where j = {1,2,3,...,N}

9. Periodically node n_S also selects MAC of message blocks $H_{(m_i+r)}$ and $f(x)_{i+r}$ and calculate C_{i+r} and sends its respective node

10. Receiver nodes n_i collects future C_{i+r}values and wait for time t_{c+r}

11. At time t_{c+r} sender again sends same $C_{i+r}$to all nodes

12. Receiver nodes decrypt both C_{i+r}values When disclosed key comes and compares the values. If both values are same then send message "data received successfully".

13. Node n_S checks labels of all node N and stops algorithm.

5. Implementation

We simulated the proposed algorithm using a custom .net based simulator. In the custom simulator software, we created different scenarios for cluster formation, routing and topology control. For topology control, we considered random deployment of nodes in the network. The snapshot gives the idea of network that is built with the system proposed.

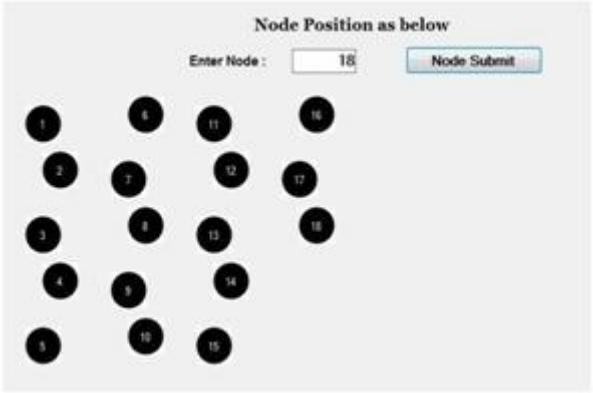

Figure 4: Dynamic network of nodes.

The message is encrypted as the user applies digital sign. Packet is transmitted as users asks for transmit.

Figure 5: Digital Signature application.

The message is encrypted as the user applies digital sign.

6. Result and Discussion

Proposed algorithm is simulated using a custom .net based simulator. In the custom simulator, Different scenarios are created for cluster formation, routing and topology control. Topology control considering random deployment of nodes in the network is achieved. The graph of nodes versus key size of our simulated network environment.

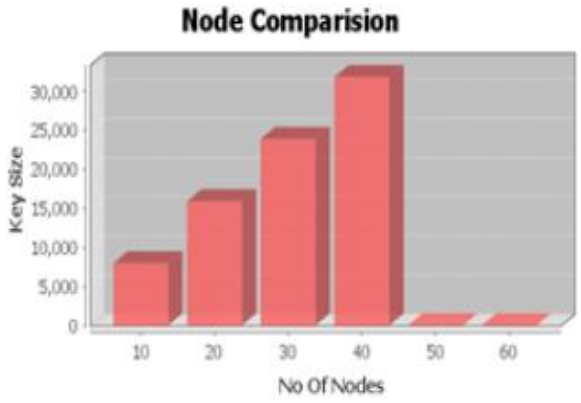

Figure 6: Graph of number of nodes Vs key size

As shown in the graph, when the number of nodes increases it results into the increase in the size of key size.

Proposed system uses a time between sender and receiver nodes to achieve asymmetry property. It associates chain of keys which are associated with a time interval. At sender's end MAC is attached to each packet which is computed on the message. sender gives a disclosure key from the key chain after a constant pre-defined time. Receiver receives the packets and stores the received packets in the buffer. Receiver knows the schedule of the key disclosure. As it gets the disclosure key receivers verifies the packets in the buffer. Each receiver checks the key in the hash of key chain and then checks the correctness of MAC. If the MAC value is correct then only the receiver accepts the packet otherwise it rejects the packet.

7. Conclusion

In recent years, mobile ad hoc networks (MANETs) have become popular, because of their easy of deployment. As single packet reaches many users it creates potential danger of malicious user, who is able to inject packet, can reach to many receivers with a malicious packet. AS nodes in network join and leave the group randomly, it becomes challenging to track them for security mechanisms. In this research work, we presented the proposed system, a scalable and light-weight mechanism to address the problems of authentication in multicast mobile ad hoc networks. It uses symmetric cryptography, and time-delayed key disclosure to achieve authenticated broadcast. Feasibility of the proposed approach can be seen by prototype implementation. Future scope of the project is to develop hop to hop connectivity and integrity.

8. Acknowledgment

I am profoundly grateful to prof. Ram Joshi for his expert guidance and continuous encouragement throughout to see that this review work rights its target since its commencement to its completion. His invaluable guidance supported me in completing this survey. At last I must express our sincere heartfelt gratitude to all staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

References

[1] Quansheng Guan, Richard Yu,"Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 6, JULY 2012.
[2] Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris, "Preventing Im- personation Attacks in MANET with Multi-factor Authentication", IEEE transactions published at Department of Informatics, University of Piraeus, Greece, 2008
[3] Qiwei Lu; Yan Xiong; Wenchao Huang; Xudong Gong; Fuyou ,"Distributed ECC-DSS Authentication Scheme Based on CRT-VSS and Trusted Computing in

MANET", Miao2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 656 665, 2012
[4] Kavitha Ammayappan, V.N.Sastry and Atul Negi, "Authentication And Dynamic Key Management Protocol Based On Certified Tokens For Manets", Institute for Development and Research in Banking Technology, Hyderabad, India, 2009
[5] Striki, M.Inst. for Syst. Res., Maryland Univ., College Park, MD, USA ; Baras, J.S."Towards integrating key distribution with entity authentication for efficient, scalable and secure group communication in MANETs", Communications, 2004 IEEE International Conference on (Volume:7)
[6] Rajaram Ayyasamy1 and Palaniswami Subramani, "An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Adhoc Networks", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012
[7] Na Ruan, Yoshiaki Hori, âAˇ IJDoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Thingsâˇ AˇI, 2012 International Conference on Selected Topics in Mobile and Wireless Networking, pp 60 65, Apr. 2012
[8] Soumyadev Maity and R. C. Hansdah, "Membership Models and the Design of Authentication Protocols for MANETs", 26th International Conference on Advanced Information Networking and Applications Workshops, pp 544-551, July 2012.
[9] Aasia Samreen and Seema Ansari," Certificateless ID-based Authentication using Threshold signature for P2P MANETs", Department of Computer Science, University of Aasia, Ireland, pp 25 30, July 2009
[10] M. Suguna, P. Subathra, "Establishment of Stable Certificate Chains for Authentication in Mobile Ad Hoc Networks"IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011
[11] Wei Liu, Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" Nov. 2014 Vehicular Technology, IEEE Transactions on (Volume:63 , Issue: 9)
[12] Jason L. Wright, Milos Manic, "Time Synchronization in Hierarchical TESLA Wireless Sensor Networks", Int. J. Comput. Sci. Netw. Security, pp 36 39, 2009.

Author Profile

Tejashree Kokate receieved the B.E degree in computer Engineering from Cummins college of Engineering (Savitribai Phule Pune University) in 2011. During 2013 -14 she worked as lecturer in Shivaji college, Barshi. She started her post graduation program at Marathwada mitra mandal college of engineering in 2013. Currently she is studying for Masters in engineering at MMCOE, Pune.