Far East Journal of Electronics and Communications
100 *Proceedings of SHANNON - 3rd Int. Conf. Comp. Sci.*, 2016
© 2016 Pushpa Publishing House, Allahabad, India
http://dx.doi.org/10.17654/ECSV3PI16001
Special Volume 3, Part I, 2016, Pages 1-12 **ISSN: 0973-7006**

MOBILE NODE AUTHENTICATION IN MANET USING ENHANCED CLUSTER BASED AUCRES ALGORITHM

Neha Sharma and Ambrish Gangal

Department of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab, India

Abstract

Mobile ad-hoc network (MANET) is a collection of mobile nodes which do not have any infrastructure, i.e., access points. Designing an efficient authentication mechanism for such a large mobile network is challenging task as the nodes have limited battery and bandwidth constraints. There are different types of attacks which consume resources of the whole network and hence disrupt the routing process. This paper proposes an authentication technique without use of any trusted third party (TTP) or Certifying Authority (CA). Clustering provides an effective way to divide network to make the areas within which routing is performed and overhead is also reduced. For mutual authentication of nodes, clustering is used with keys and unique identity numbers together provides authentication and the cluster heads will account for mobility. This will restrict the malicious nodes to enter into the network and thus reduces the chances of attack.

1. Introduction

Mobile ad-hoc networks (MANETs) consist of self organizing nodes with high mobility that communicates via nodes itself. Unlike traditional

Conference held during April 8-9, 2016 at Lovely Professional University, Punjab, India.
Guest Editor: G. Geetha; Division of Research and Development, Lovely Professional University, Punjab, India.

networks which used wired systems and fixed infrastructure, MANETs do not have fixed infrastructure which means that it does not have base stations and centralized management points. MANETs are characterized on the basis of various features that calculate for the mobility of the nodes inside the network: battery life, infrastructure less, dynamic topology, multi-hop routing, distributed nature and many more. Self organizing nature of the nodes makes them viable for virtual conferences, battlefield applications, remote unmanned sensor networks, military purposes as compared to the fixed infrastructure used by the traditional networks where dedicated nodes are used for packet forwarding.

Due to its open nature, MANET is prone to various attacks. Attacks include various passive attacks like eavesdropping, modifying, replaying the message [1]. Some nodes can behave maliciously while being in the network so that it may not be possible to identify them easily. Such nodes advertise false routes and provide incorrect update information therefore affecting network and leading to a byzantine failure. Various secure routing protocols are proposed to enhance the network security. One major pitfall is that all those routing protocols assume to be secure channel by which link can be made between the sender and the receiver. But for such a secure systems, security associations (SA) must be made first by both the parties involved in the transmission. Clustering techniques are applied to make an effective way for routing which reduces overhead. Clustering is also now-a-days used to provide authentication. Various algorithms are proposed some of them include LIC, HCC, K-CONID and many more [2].

In this paper, an efficient framework for authenticating nodes inside MANET is proposed that can easily provide a way to identify the malicious node. The main solutions of this paper focus on following problems in existing methodologies: (i) use of TTP (trusted third party), (ii) public-private key pair and (iii) authenticating malicious nodes. This paper solves the above mentioned problems efficiently. The rest of paper is organized as

follows: Section 2 provides the related work in the field of authentication. Section 3 presents the proposed framework for authentication. Section 4 concludes the paper and also provides future scope of the work to improve it further.

2. Related Work

The most challenging task in MANET is to provide security. Security aspects include authentication, confidentiality, availability and integrity. Authentication is the major problem in MANETs. Cryptography and key exchanges are well known techniques for this problem.

Zhou and Hass [3] first proposed threshold cryptography based key management technique for MANET. Total of *n* nodes have the share of master secret key which is generated using threshold cryptography. Thus any node that needs to join the network must first obtain all *n* partial signatures to form a complete signature for accessing the network resources. The major drawback of this scheme is the risk of disclosure of key. If the malicious nodes get access to all the *n* keys, then it can easily form a certifying authority and can issue certificates.

Sen [4] proposed a Robust and Efficient Node Authentication Protocol for MANETs. Nodes here are authenticated mutually. Before entering the network the node generates public/private key pair. This key exchange protocol used the CREQ (certificate request) packets method, adopted in reactive protocols, which here was used for retrieving the public keys of the nodes. To make the protocol efficient, two approaches are taken: (a) multi-path certificate exchange and (b) trust-based certificates. Three operations are described. Initialization, certificate exchange and certificate revocation. But many spurious certificates can be generated which may prove fatal for the network.

Hashmi and Brooke [5] gave different authentication techniques: Centralized CA distributed CA, self CA systems and hybrid schemes.

Problems with all these techniques are listed in the table as following:

Table 1. Comparison of authentication mechanisms

Authentication Mechanism	Problem
Central CA	Infrastructure cost is high
Distributed CA	Malicious node can Acquire multiple IDs
Self CA	Arbitrary identities are created by the nodes themselves
Hybrid • MANET-ID • Multiple-key Cryptography	TTP is required for bootstrapping phase Sybil attack is possible

Kaur et al. [6] proposed weightage based secure energy efficient clustering algorithm in which rely factor $(RF_{\alpha,\beta})$ is calculated based on the behavior of nodes and compared with a threshold value. CH is elected with the weights values. Bechler et al. [7] introduced a cluster based architecture in which arbitrary nodes with warranty certificates warrant a new node's identity. Arbitrary nodes can be compromised. Bednarczyk and Gajewski [8] proposed a clustering algorithm based on various parameters like battery level, stationary factor, received power level known as weights. Gomathi and Parvathavarthini [9] used direct trust evaluation and gave trust value of a node which is compared with a predefined threshold value. It contributed a trusted environment for mobile nodes.

Komninos et al. [10] proposed a layered security approach which helps in securing ad-hoc network using authentication protocols. In the first phase the nodes try to authenticate to determine the identity by sing challenge response protocols which are totally based on symmetric key techniques. In second phase again nodes authenticate based on challenge response with the help of public key cryptography.

Devi and Arunmozhi [11] proposed CBAS method to improve the security of MANET. Authentication uses zero knowledge protocol (ZKP) in which the secret key is never directly passed master head node deletes the attacker node and then the communication starts. It improved the

performance but consumes more energy. Thus an energy efficient approach is needed. Aruna and Subramani [12] provides study of waited clustering algorithms which includes single metric based clustering and multiple metrics based clustering that involves WCA (weight based clustering algorithm), WBACA (weight based adaptive clustering) and many more. Based on the comparisons between these algorithms, multiple metric based clustering proves to be more efficient.

Govil et al. [13] proposed a technique for selecting cluster head based on the energy level and hence conserving the energy in the network. It considers the battery power capacity (BPC), residual battery power (RBP) and distance. CH is selected in the cluster of m mobile nodes. Yang [14] reviewed different techniques for authentication and gave a mechanism. A multi-step authentication process is proposed which proves to be better for identifying nodes. Node which had the maximum confidence value is chosen as a CA which issues certificates to each cluster head. The CH issues authentication key to the nodes by checking the reliability factor of nodes. But it involves two entities one a CA and other CH which will increase the overhead over the system and also the confidence value is somewhat susceptible to changes by the malicious node.

Dhurandher et al. [15] proposed a friend based authentication scheme which provides efficient mechanism to broadcast information about the trusted nodes in the network. It establishes trust through friends and uses challenges based message for authentication. This provides an efficient and robust method for secure authentication.

Murugesan et al. [16] proposed a node authentication clustering based security for ad-hoc networks. It used location of node (x, y) as the key pair for that node and used it for authentication. The problem with type of authentication is that it involves location as a deciding factor for authenticating which can easily be spoofed and hence any node can get information of other nodes and use that location as a key pair.

3. Proposed Work

The proposed work integrates the clustering and authentication algorithm which proves to be useful in limiting the access to resources for the malicious nodes which wants to enter the network.

A. Framework

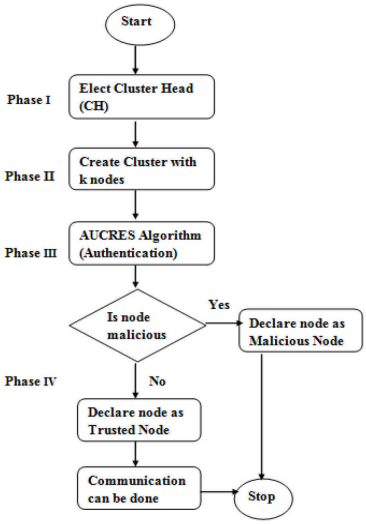


Figure 1. Framework for authentication.

Different phases conclude the framework as shown in Figure 1. Each phase in its own is an algorithm. Phases are explained as below:

Phase I: Cluster head election

In the initialization phase first the weights are computed and cluster head is elected. For this EDWCA [17, 18] is used.

1. Weight calculation

All the nodes broadcast its ID, assigned at the beginning to all the nodes, to one hop neighbors and each node involves some calculation to know their weights based on the above mentioned metrics.

EDWCA executes clustering based on these parameters. Weight W_i is calculated as:

$$W_i = a * E_i + b * D_i + c * d_i \quad (1)$$

E_i = Energy level in the node i

D_i = Distance from the neighbor node i

d_i = Degree difference of node i

where a, b, c are the coefficients.

2. Cluster head election

After the nodes calculated their weights as in (1) will now broadcast the information to all 1-hop neighbors and will compare the weights of all the nodes. The node with highest W_i will be selected as CH as shown In Figure 2.

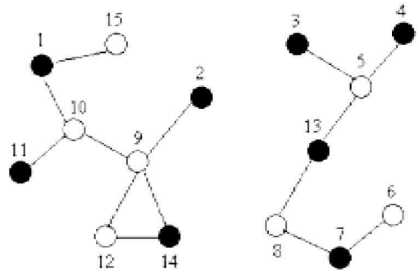


Figure 2. Cluster head election.

Phase II: Cluster formation

After the CH election, the neighboring nodes will send the message "I want to be a member of this cluster". The node which gets the response of more than one CH will act as a gateway node and all others as members. Figure 3 depicts different clusters formed.

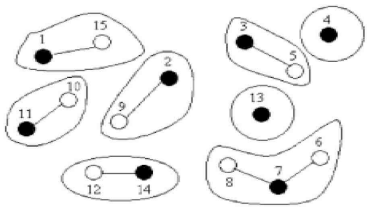


Figure 3. Cluster formation.

Phase III: AUCRES generation algorithm

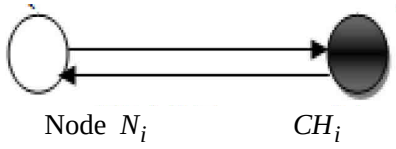
After the nodes enter into the cluster the nodes will be authenticated by the cluster head. Process of authentication is as follows:

1. Authentication mechanism

Step I. Node provides its MAC address to the CH and CH will provide a corresponding 48 bit random address or a number to the node using an encrypted channel which it will store in a table. Thus identity of the node is kept with the CH. Each node has to register itself after entering the network as shown in Figure 4.

(MAC Address + Node ID)

(48 bit R_i mapped to address)

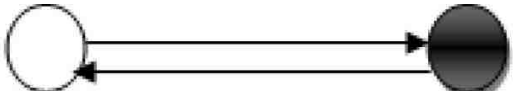


Node N_i CH_i

Figure 4. Request identity.

Step II. Both node and CH execute the AUCRES authentication algorithm using a 128 bit random key K_i for cluster 'i' and generate 32 bit AUCRES (authentication response) as shown in Figure 5.

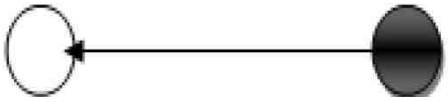
32 bit AUCRES



(32 bit AUCRES)

Figure 5. Response generation.

Step III. If 32 bit response matches from both the node and the cluster head CH, then the node is authenticated and allowed to enter the network otherwise is simply declared as unauthenticated. Figure 6 depicts the same.



(AUTHENTICATED)

Figure 6. AUCRES generation algorithm.

2. AUCRES generation algorithm

This algorithm generates a 32 bit authentication response as shown in Figure 7. It uses a 128 bit random number which is distributed by the CH to all the nodes and a 128 bit padded random address (called as unique key in Figure 8) mapped to MAC address of the node provided at the initialization phase of the authentication. It is cryptographically secure because of the key size.

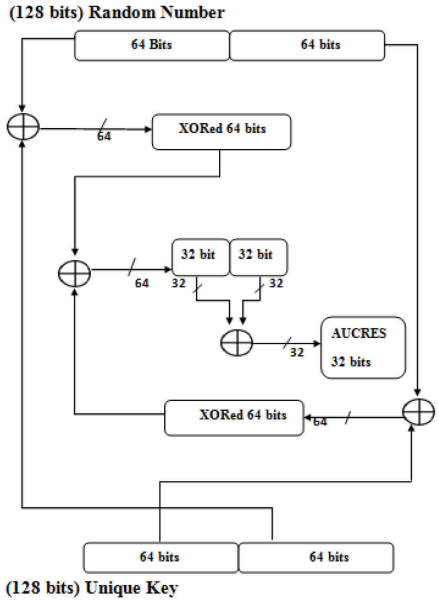


Figure 7. 32-bit AUCRES generation.

B. Mobility phase authentication

Cluster member movement

When cluster member moves out from the cluster '*i*' and comes in vicinity of other cluster '*j*'. The CH of cluster '*j*' confirms the nodes authentication in previous cluster '*i*' from CH_i not with the node itself as shown in Figure 7. This will provide a secure and efficient way of authentication.

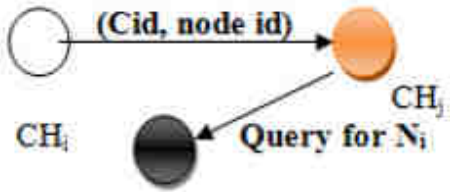


Figure 8. CH_i-CH_j communication.

Cluster head movement

There may be a case when cluster head moves away. So before leaving, CH searches for the node with maximum remaining battery power in its neighbor table and hand over all the tables to that node, thus forming a new cluster head in situation of movement.

4. Conclusion and Future Work

The security is of major concern when nodes move from one cluster to another. The algorithm provides communication between the CHs rather than the CH and the node, hence reducing overhead of node-node communication. Thus the algorithm proves to be effective as the ID it uses is unique and cannot be intercepted. Key is 128-bit long which itself is much secure as compared to other similar works. No use of TTP prevents the authentication system to rely on a single entity. Hence the system is more efficient in providing authentication.

Single point of failure is always the point in MANET as there are no

access points (APs). Our future work will be focusing on this aspect. Furthermore transmission of the keys through a secure channel is of great importance considering security issues in mobile networks. In future this aspect will be dealt to enhance the security of the authentication mechanism.

References

[1] P. Veeraraghavan and V. Limaye, Security Threats in Mobile Ad Hoc Networks, 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 2007, pp. 1-22.

[2] R. Xu, Survey of clustering algorithms for MANET, IEEE Transactions on Neural Networks 16(3) (2005), 645-678.

[3] Z. J. Haas, Securing ad hoc networks, IEEE Netw. 13 (1999), 24-30.

[4] J. Sen, A Robust and Efficient Node Authentication Protocol for Mobile Ad Hoc Networks, 2010 Second International Conference on Computational Intelligence, Modelling and Simulation, 2010, pp. 476-481.

[5] S. Hashmi and J. Brooke, Authentication Mechanisms for Mobile Ad-Hoc Networks and Resistance to Sybil Attack, 2008 Second Int. Conf. Emerg. Secur. Information, Syst. Technol. 2008, pp. 120-126.

[6] K. Kaur, J. Singh and Himani, Weightage based Secure Energy Efficient Clustering Algorithm in MANET, 2015 International Conference on, *Kochi*, Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 1006-1012.

[7] M. Bechler, H. Hof, D. Kraft, F. Pählke and L. Wolf, A cluster-based security architecture for ad-hoc networks, INFOCOM 2004, 23rd Annu. Conf. IEEE Comput. Commun. Soc. 2004, pp. 2393-2403.

[8] W. Bednarczyk and P. Gajewski, An enhanced algorithm for MANET clustering based on weighted parameters, J. Commun. Network 1(3) (2013), 88-94.

[9] K. Gomathi and B. Parvathavarthini, A Secure Clustering in MANET through Direct Trust Evaluation Technique, 2015 International Conference on, Riyadh, Cloud Computing (ICCC), 2015.

[10] N. Komninos, D. Vergados and C. Douligeris, Layered security design for mobile ad hoc networks, Comput. Secur. 25(2) (2006), 121-130.

[11] C. S. Devi and S. A. Arunmozhi, Cluster based Authentication Scheme (CBAS) for Secure Routing in MANET, Internet. J. Comput. Appl. 121(8) (2015), 36-41.

[12] S. Aruna and A. Subramanian, Comparative Study of Weighted Clustering Algorithms for Mobile Ad Hoc Networks, International Journal of Emerging Technology & Advanced Engineering (IJETAE), 4(5) (2014), 307-311.

[13] K. Govil, S. K. Gupta and A. Agarwal, Cluster Head Selection Technique for Optimization of Energy Conservation in MANET, 2014 International Conference on Parallel, Distributed and Grid Computing (PDGC), 2014, pp. 39-42.

[14] H. Yang, Authentication Techniques for Improving the Reliability of the Nodes in the MANET, International Journal of Multimedia and Ubiquitous Engineering 10(7) (2015), 277-284.

[15] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, FACES: Friend-based Ad hoc routing using challenges to establish security in MANETs systems, IEEE Syst. J. 5(2) (2011), 176-188.

[16] R. Murugesan, M. Saravanan and M. Vijyaraj, A Node Authentication Clustering Based Security for ADHOC Network, 2014 International Conference on Communications and Signal Processing (ICCSP), 2014, pp. 1168-1172.

[17] K. Gomathi and B. Parvathavarthini, An Enhanced Distributed Weighted Clustering Algorithm for Intra and Inter cluster routing in MANET, International Journal of Innovative Research in Compute and Communication Engineering 2(12) (2014), 7566-7572.

[18] M. Chatterjee, S. K. Das and D. Turgut, WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks, Journal of Cluster Computing 5(2) (2014), 193-204.