Cryptanalysis of Secure Routing Among Authenticated Nodes in MANETs

Rajeev Ranjan

Abstract Secure routing (SR) is one of the most important issues in Mobile Ad hoc Networks (MANETs). Recently, in 2013, Zhao et al. proposed an efficient routing integrated framework for MANETs. They claimed that their proposed scheme distributes the system parameter only to the authenticate nodes before network set up phase. However, based on cryptanalysis, we have found that an unauthenticated nodes are also be able to get that original system parameter and behave like a malicious node in the network. Thus, their scheme fails to provide an authenticate distribution mechanism in real life application. As a counter measurement, this paper aims to present an efficient authenticated distribution mechanism that can be incorporated very efficiently in their scheme. Our proposed technique is found to be secure under the hardness of Computational Diffie-Hellman (CDH) assumption.

Keywords Secure routing · MANETs · Security attacks · Authentication technique · Routing protocols

1 Introduction

In the current decade, mobile ad hoc networks (MANETs) have received more and more attention because of their capabilities of self-maintenance and configuration. MANETs is a system of wireless mobile nodes which dynamically self-organize in arbitrary and temporary network topologies. In MANETs nodes may be mobile phones, computer, laptop, personal digital assistants (PDA) and handheld digital devices etc. MANETs doesn't have any fixed infrastructure, i.e. there is no base station. Mobile ad hoc network structure shown in Fig. 1. Nodes arbitrarily change their own position resulting in a highly dynamic topology causing wireless links to be broken and re-established on the fly. The deployment of such networks faces

R. Ranjan (✉)
Department of Computer Science and Engineering,
Indian Institute of Technology (ISM), Dhanbad 826004, India
e-mail: rajeev.macet@gmail.com

S.C. Satapathy et al. (eds.), *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, Advances in Intelligent Systems and Computing 516, DOI 10.1007/978-981-10-3156-4_23

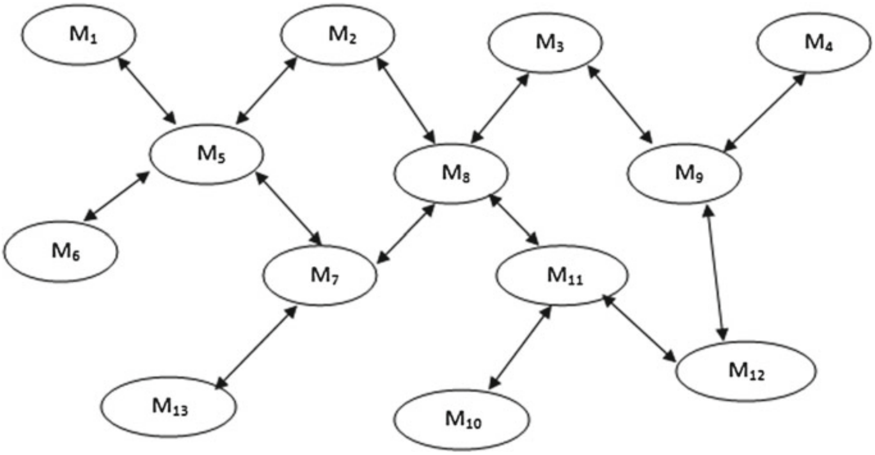

Fig. 1 Mobile ad hoc network (MANETs)

many challenges such as limited physical security, node mobility, low processing power, low bandwidth and limited memory storage capacity. MANETs is used in such field like Emergency search operation, rescue operations, disaster relief effort, mine site operations, military operations in battle fields, electronic classrooms, conferences, convention centers etc. [1]. In MANETs, nodes can directly communicate with other neighbor nodes within radio-ranges; whereas nodes that are not in the direct communication range use the intermediate node to communicate with each other. In both situations, all the participated nodes in the communication automatically form a wireless network, therefore this kind of wireless mobile network is called as a mobile ad hoc network. Compared to the wired networks and MANETs, MANETs are much more vulnerable for security attacks.

This is mainly due to its features of not closed medium, active topology, cooperative algorithms, lack of centralized supervise and management point. Secure routing is a progressive research area in ad hoc network and recent years, several routing protocol has been proposed for MANETS [2–5]. Current research is going on to secure routing and communication in MANETs. For security reasons MANETS should be expected to meet the following different security requirements [6].

Confidentiality: Only the knowing receivers should be able to execute the transmitted data.

Integrity: Before and after the transmission process data should be modified. It is ensured that data integrity must be maintained. i.e. during the transmission process the data should be entact.

Availability: The term availability refers that information should be available for legitimate nodes or authorized parties when needed.

Authentication: Authentication is a method to check the message coming from authentic node or authorized party or not. Nodes are able to authenticate the data has been sent by the authorized node.

Non-repudiation: Non repudiation is a process by which sender of a message cannot deny the sending the message and also receiver cannot deny the receipt after receiving the message. In recent years, many routing protocols have been proposed by researchers for MANETs. These routing protocols are proactive (Table driven) [7, 8], reactive (on demand) [9, 10] and Hybrid routing protocols [11]. The lists of well-known routing protocols are categories in Fig. 2.

Reactive routing protocol: It is a on demand routing protocol, when route is required node flooded the route request message and find the route. After that source route sends the message to the destination node.

Proactive routing protocol: In proactive or table driven routing protocols, every node maintains the network topology information in the form of routing tables by sending HELLO messages periodically. If the link is not broken, then both the nodes exchange their routing information.

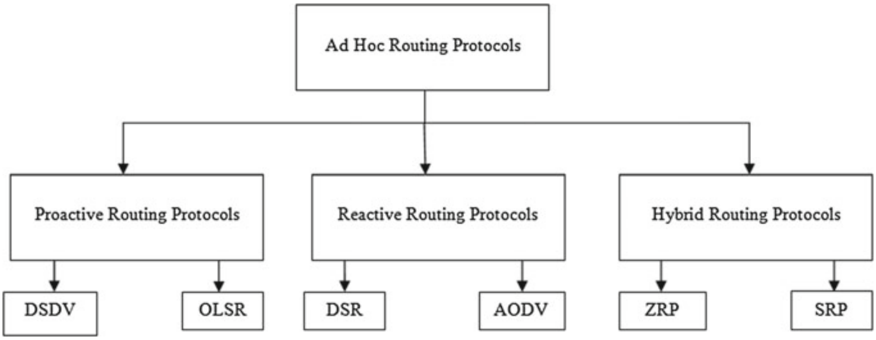

Fig. 2 Classification of routing protocols

Table 1 List of notations used

Symbol	Description
Z	Finite integer set
Z_n	Set of integer after modulo n
F_q	q elements with finite fields
Z_q^*	The multiplicative group of integers modulo prime number q
E/F_p	Elliptic curve over finite field (F_p)
d_{id}	Private key corresponding to node identity
Q_{id}	Public key corresponding to node identity
S	Secret key (Master)
P_{pub}	Public key (System)
H_i	An i, integer usage as subscript, in the system multiple hash function are used
G_1	The additive group, sub group of points on E/F_p
G_2	The multiplicative group, subgroup of the finite field
P, Q	Two points on elliptic curve

Hybrid routing protocol: Hybrid routing protocols are protocols that combine the best features of both reactive and proactive routing protocols.

In this paper we used IBE technique and same system parameter used in Boneh-Franklin's IBC scheme [12, 13]. The notations used in this scheme are summarized in Table 1. For the setup of system parameter a PKG is required for IBC cryptosystems. The system public key (P_{pub}) setup by PKG. $P_{pub} = sP$, where s is any number belongs to Z_q^* and P is a point on elliptic curve (E/F_p).

2 Review of Authentication Phase in Zhao et al. Routing Protocol

The authentication technique used in Zhao et al. protocol [14] is as follows:

- The PKG selects a random $s_0 \in Z_q^*$ and $P_0 \in E/F_p$ of order q, and distributes pseudo system parameters $params = < p, q, P_0, P_{pub0}, H, H_0, H_1 >, (P_{pub0} = s_0 P_0)$ through public channels as traditional IBC schemes do.
- Nodes demands to private keys and real system parameters. Node A selects a random x_A in Z_q^*, encrypts its identity ID (with proof) with $K_A = e(x_A.P_{pub0}, P_0)$ and sends the encrypted identity C_{ID} with $x_A P_0$ to the PKG: $< C_{ID}, x_A P_0 >$.
- The PKG decrypts ID with $k_0 = e(s_0.(x_A P_0), P_0) = K_A$, authenticate identity of node A. The parameter P, P_{pub} and As private key with k_0 encrypts updated system if that gets through it and through public channels, it is sent back to the respective node. Then updated system parameters and its private key is decrypted by node A. Other node which is not aware of x_A cannot learn that information.

3 Attack on Authentication Phase in Zhao et al. Routing Protocol

It is found that Zhao et al. scheme is insecure under Key compromisation attack. That is, a node is able to generate the key and read and/or modify the message during the communication. Other node which is not aware of x_A cannot learn that information. The process is as follows:

- Sender node(A) is sending $< C_{ID}, x_A P_0 >$
- Attacker interrupt the message and collect $V = x_A P_0$ and can able to compute the symmetric secret key $k_A = e(V, P_{pub0}) = e(P_0, P_0)^{x_A s_0}$

Thus, not only authenticated nodes, but also attacker are able to compute the secret key, and thus the whole process is under attack.

4 Proposed Authentication Technique

The process is similar to the previous system. Additionally, we choose another point Q in E/F_P and make $params = < p, q, P_0, Q, P_{pub0}, H, H_0, H_1 >$, $(P_{pub0} = s_0 P_0)$ through public channels as did in previous system. Nodes apply to real system parameters and private keys. A node A selects a random r in Z_q^*, encrypts its identity ID (with proof) with $k = e(P_{pub0}, rQ)$ and sends the encrypted identity C_{ID} with rP_0 to the PKG: $< C_{ID}, rP_0 >$

$$K = e(P_{pub0}, rQ) = e(s_0 P_0, rQ) = e(P_0, Q)^{rs_0} \tag{1}$$

$$C_{ID} = AES(K, ID_A) \tag{2}$$

The PKG decrypts ID with $K_0 = e(s_0.Q, (rP_0)) = K$, authenticate identity of node A. The parameter P, P_{pub} and private key of node A with k_0 encrypts updated system if that gets through it and through public channels, it is sent back to the respective node. Then updated system parameters and its private key are decrypted by node A.

$$K_0 = e(rP_0, s_0 Q) = e(P_0, Q)^{rs_0} \tag{3}$$

If $K = K_0$, verifies identity of node A after that PKG updated system parameter P, P_{pub} in place of P_0 and P_{pub0} it is sent back to the respective nodes through public channels. The updated new system parameter is $< p, q, P, Q, P_{pub}, H, H_0, H_1 >$.

Now nodes are authenticated for secure communication. We choose proactive routing protocol OLSR because it has high efficacy, flexibility and extensibility for secure communication in MANETs.

5 Security Analysis

Definition (*Computational Diffie-Hellman Assumption*) For an algorithm A, the computation of $Z = b.Q$ in polynomial time t from the given tuple $< P, Q, bP >$ is very hard, where b is chosen at random.

Theorem *The proposed authentication scheme is secure under the hardness of CDH assumption, i.e., if the scheme is breakable then the underline hard problem is solvable in polynomial time.*

Proof Here we show that due to the unavailability of r other nodes cannot learn the corresponding information due to the hardness of CDH assumption which was leaked in Zhao et al. authentication technique. Unlike their scheme, we have introduced another point Q in E/F_p and resist the previous attack, i.e., a malicious node can also behave as original node and read as well as modified the message due to the valid secret key. Here, in attacker point of view, the hardness of finding a solution is to compute $Z = s_0Q$ from the given tuple $< Q, P_0, s_0P_0 >$ for an unknown $s_0 \in Z_q^*$. If it is solvable then an attacker is also able to generate the symmetric key$K = e(P_0, Q)^{s_0}$ and decrypt any message by acting as an authentication node. Since, there is no solution exists in polynomial time for the CDH problem, so, our authentication technique is secure as long as CDH is hard.

6 Conclusion

Recently, Zhao et al. proposed an efficient routing technique. For this, they have given a proposal of an authentication technique. However, we show that their proposed authentication technique is not secure in real time attack. So, as an enhancement, we have proposed an efficient authentication technique which is suitable for Zhao et al. routing scheme. The proposed technique is found to be secured under the hardness of CDH assumption.

References

1. P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in *Advanced communications and multimedia security* (Springer, 2002), pp. 107–121
2. S. Buchegger, J.-Y. Le Boudec, Performance analysis of the confidant protocol, in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* (ACM, 2002), pp. 226–236
3. D. Coppersmith, M. Jakobsson, Almost optimal hash sequence traversal, in *Financial Cryptography* (Springer, 2002), pp 102–119
4. Ralf Hauser, Tony Przygienda, Gene Tsudik, Lowering security overhead in link state routing. Comput. Netw. **31**(8), 885–894 (1999)
5. D.B. Johnson, Routing in ad hoc networks of mobile hosts, in *First Workshop on Mobile Computing Systems and Applications, WMCSA 1994.* (IEEE, 1994), pp. 158–163
6. W. Su, M. Gerla, Ipv6 flow handoff in ad hoc wireless networks using mobility prediction, in*Global Telecommunications Conference, 1999. GLOBECOM'99*, vol. 1 (IEEE, 1999), pp 271–275
7. T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, Optimized link state routing protocol (olsr) (2003)
8. C.E. Perkins, P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers, in textitACM SIGCOMM Computer Communication Review, vol. 24 (ACM, 1994), pp. 234–244
9. D.B Johnson, The dynamic source routing protocol for mobile ad hoc networks. *draft-ietf-manet-dsr-09.txt* (2003)
10. E.M. Royer, C.E. Perkins, Multicast operation of the ad-hoc on-demand distance vector routing protocol, in *Proceedings of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking* (ACM, 1999), pp. 207–218
11. Z.J. Haas, M.R. Pearlman, P. Samar, The zone routing protocol (zrp) for ad hoc networks (2002)
12. D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in *Advances in Cryptology CRYPTO 2001* (Springer, 2001), pp. 213–229

13. Muhammad Bohio, Ali Miri, Efficient identity-based security schemes for ad hoc network routing protocols. Ad hoc Netw. **2**(3), 309–317 (2004)
14. S. Zhao, R. Kent, A. Aggarwal, A key management and secure routing integrated framework for mobile ad-hoc networks. Ad Hoc Netw. **11**(3), 1046–1061 (2013)