Wireless Pers Commun (2015) 81:1031–1043
DOI 10.1007/s11277-014-2169-1

Mutual Authentication and Updating the Authentication Key in MANETS

Ahmad Alomari

Published online: 8 November 2014

Abstract Mobile Ad hoc Networks (MANETs) are new wireless networks with a self-configuring and self-maintaining topology, also characterized as dynamic topology. The architecture in MANETs has been introduced few years ago and its main characteristic is that it does not rely on any fixed infrastructure. These features bring in security vulnerabilities and also make it difficult to ensure security services to MANETs. To counteract this problem major research has been done. This article will talk about the approaches that intend to develop security schemes to MANETs and to create a defense against various attacks at different layers. Routing is a very important function in MANETs. It can also be easily misused, leading to several types of attack. This article proposes a scheme to improve and support mutual authentication and encrypt communication between the nodes in the MANET. The authentication scheme proposed is seeking to solve the security and privacy issues between any two communicating nodes in the MANET.

Keywords MANETs · Routing protocol · Authentication key · Random number

1 Introduction

A mobile ad hoc network (MANET) is a group of wireless mobile nodes forming a precarious network without the aid of any established infrastructure or centralized administration. Opposed to any conventional wired networks, the MANETs have no fixed infrastructure (base stations, centralized management points and the like). This kind of network is a new type of self-organizing network which combines wireless communication with a high-degree node mobility and forms union of nodes with an arbitrary topology [1].

Because the nodes are mobile, network topology may change unpredictably and rapidly over time. Decentralized network: all network activity, including the discovery of topology and delivery of messages, must be executed by the nodes themselves. In [2] and [3], it

A. Alomari (✉)
Faculty of Mathematics and Computer Science, University of Bucharest, Bucharest, Romania
e-mail: alomari.jordan@gmail.com

has been suggested threshold encryption to provide reliability, the main distribution of key management for MANET through the exploitation of some of the nodes as an anchor of confidence for the rest of the network.

MANET security is an essential element for the basic network functions such as packet forwarding and routing. Network operation can be easily attacked if it does not include countermeasures to the basic network functions in the early stages of design. Unlike ad hoc networks using the nodes to support the basic functions such as packet forwarding, routing and network management, ad hoc networks carry out those functions by all nodes available. This difference is at the very essence of the security problems that are specific to ad hoc networks. In contrast to the nodes of the classic network specialist, the nodes of an ad hoc network cannot be trusted for the correct implementation of the critical network functions. We can classify security MANET in five layers, such as the application layer, transport layer, network layer, link layer, and physical layer.

However, the layer that deals only with security issues is the network layer, so we only focus on it to protect directing of the ad hoc routing protocols. From the standpoint of security design, the MANETs do not have a clear line of defence [4]. Unlike wired networks dedicated routers, each node in the ad hoc mobile network may act as a router and forward packets to other peer nodes. Routing in Ad Hoc networks became a popular search topic. Dating back to the early 1980s, there was a large number of routing protocols designed for multi-hop peer ad hoc networks. Various routing protocols for ad hoc networks have been developed to produce a secure environment between the nodes. In our schemes we can apply this in the most types of the routing protocols such as the reactive and proactive routing protocols that we focus in this paper. The structure of a MANET consists in mobile nodes which can act as a sender and a forwarder which is used for messages. Our accent will be put on the unique feature of these protocols, feature which is represented by the ability to trace routes in spite of dynamic topology. The attacks which can occur on ad-hoc network can be passive attacks and active attacks.

In this paper, security in mobile ad-hoc networks represents a fold problem. The first is represented by the nodes' communication security of the routing and the second problem refers to protection of the data which is traveling through the network on routes established by the routing protocols.

2 Types of Ad-Hoc Routing Protocols

There are basically two types of ad hoc routing protocols (as appear in Fig. 1).

2.1 Proactive Routing Protocols

Proactive routing protocols, where the nodes keep the routing tables updated by sending messages periodically. We have, for example, destination-sequenced distance vector (DSDV), Global State Routing (GSR) and Optimized Link State Routing Protocol (OLSR).

2.1.1 Destination-Sequenced Distance Vector

The algorithm DSDV [5] is a modified Bellman Ford routing algorithm with some improvements. All mobile nodes keep a routing table which contains different data needed for the routing process: all available destinations, how many nodes need to be passed to arrive to the destination and the sequence number allocated by the transmitter. The later is necessary in

differentiating the old routes from the new ones, which keeps the loops from forming. From time to time the nodes send their routing tables to the next-hop neighbors. All this mechanism ensures only one path to the destination.

The updates of the routing table are forwarded using two kinds of packets, in an attempt to limit the amount of overhead transmitted. The first way in which a routing table is sent is by using a "full dump". The second is the incremental update. The available routing data is transported by the full dump packet. However, the incremental packet only transports the altered data from the last full dump. If the incremental packet has enough room it might take on entries with altered sequence number. The incremental packets are forwarded more often than the full dump packets, but, because the network is dynamic, their size can get too large. In this case, the frequency with what the full dump packets are sent will be increased.

As stated before, beside the routing table data, every route update packet has a single sequence number allocated by the destination node. Most of the times, the utilized route is the one marked with the highest sequence number. In the uncommon situation where the sequence numbers are equal, the best metric route is chosen. Mobile nodes can assess routes' settling time, grounded on their previous history. They use this feature for computing how much a transmission can be delayed. The delay appears when the removal of some updates is needed, updates that appear if a better route is discovered.

2.1.2 Global State Routing

Broadly based on the traditional Link State algorithm, the GSR protocol [6] works with improved information broadcasting an outcome of the restriction of the update messages between intermediate nodes only. In Link State algorithm each node maintains a Neighbor list, a Topology table, a Next Hop table and a Distance table: the neighbor list of a node (as the name says) includes all the nodes that can be heard by a node; the topology table comprises the link state information as reported by the destination and the timestamp of the information for every destination node; the next hop to which the packets of each destination must be forwarded are contained in the next hop table; finally, the shortest distance to every destination node is included in the distance table.

The routing messages are generated on a link change as in link state protocols. The topology table is updated when receiving a routing message only if the sequence number of the message is newer than the sequence number already stored in the table. Finally, the routing table is reconstructed and the node broadcasts the information to its neighbors.

2.1.3 Optimized Link State Routing

Like in the case of the Global state routing, the OLSR [7] is also based on the traditional link-state algorithm. In this point-to-point routing protocol the link-state messages are shifted periodically, thus enabling nodes to keep topology information about the network. The innovation brought by OLSR is the employment of multipoint replaying (MPR) strategy that it minimizes the size of each control message and the number of rebroadcast nodes during each route update. This is achieved by the retransmission of packets through a set of one node's neighbors called the multipoint relays. Nodes outside the set can read and process each packet but cannot retransmit. The MPRs are selected when each node periodically disseminates a list of its one hop neighbors using hello messages.

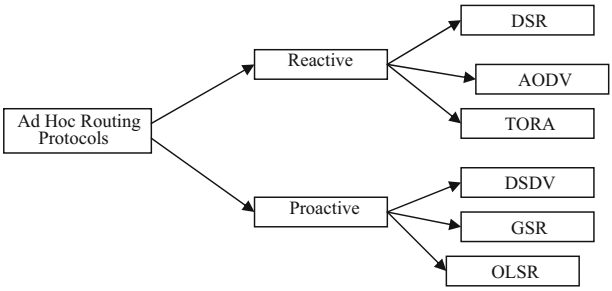

Fig. 1 Types of ad hoc routing protocols

2.2 Reaction (On Demand) Routing Protocols

Reaction (On Demand) routing protocols, where routes are created only when needed. We have, for example, Dynamic Source Routing Protocol (DSR), TORA (Temporally ordered routing algorithm) and AODV (Ad hoc demand distance vector routing protocol), as shown in Fig. 1.

The difference between these protocols is shown in the way the routing information is updated, the detection of the type of information contained in each routing table. Furthermore, each routing protocol may maintain different number of tables.

2.2.1 Dynamic Source Routing

Dynamic source routing (DSR) [8,9] is based on demand, which in its turn is founded on the theory of source routing rather than table-based. This protocol is the origin of the initiative instead of hop-by-hop. The route caches containing track sources are maintain by the mobile nodes. This design is needed precisely in multi-hop wireless networks dedicated mobile nodes. Basically, DSR protocol, as in the On-Demand routing, has no need of any network infrastructure or management, allowing the network to be completely self-organizing and self-configured. Protocol consists of two main phases: the discovery of the road and road maintenance. Each node keeps a cache to store recently discovered paths. When a packet needs to be sent to a destination, the cache route is checked first to see if that path does not already exist. If the path exists, this route is used to transport the package and also attach the source address on the package. If the path to the destination is not in the cache, a route request packet is broadcasted to all the neighbors of the sender node asking for that path. This application contains the track of the destination address, along with a unique identification number and the source node address. Each node receiving the package checks whether it knows the route to the destination. If it does not, it adds its own title to the track record package which is forwarded to its neighbors. The road is created when one node replies to a request up the road with the same destination, or an intermediate node in the cache contains the remaining track route to the destination. By the time it reaches the destination or the intermediate node's package, the request contains a route record of hops taken. Therefore, it will supervise the route maintenance process continuously and will also notify the contract if there is any failure in the path. Accordingly, the nodes change entries from the cache route.

2.2.2 Ad Hoc On-Demand Distance Vector

AODV [10] is to improve the destination sequence distance vector routing protocol (DSDV) that is based collectively on DSDV and DSR. It aims to reduce the requirements of system-wide broadcast to the fullest extent. It usually reduces the number of required broadcasts by creating routes on a demand basis, while the DSDV algorithm maintains a complete list of paths. It does not maintain the routes of each node but it discovers them when needed and retains them only as long as they are required. AODV has two main phases: route discovery and route maintenance.

Route Discovery

When the source node S wants to send a data packet to the destination node D, the routing table entries are verified to check if there is a current path to the destination node or not. If such a path exists, data packets are routed to the appropriate next hop toward the destination. If there is not a route, the path must be discovered through request messages broadcasted (RREQ) to its neighbors. This application contains guidance on its IP address, current sequence number, destination IP address, destination last sequence number and broadcast ID [11].

This operation is repeated until the RREQs reach the destination node. When it receives the first arrived RREQ, the destination node creates and sends a route reply (RREP) to the source node through the reverse path from where the next RREQ came. If the same RREQ arrives later it will be ignored by the destination node. In addition, AODV enables intermediate nodes to generate and send RREP to the source node, with destination sequence number equal to or greater than those in the RREQ.

Route Maintenance

A discovered route between a source node and destination node is maintained as long as needed by the source node. There is no movement of the nodes in the MANET. So, if the source node moves during an active session it can be seen as a mechanism for the renewal of its route or for the discovery of a new one. Whenever a broken link is discovered between two nodes the route maintenance phase is implemented. The broken link is detected by monitoring a malicious node or the whole link. The node that discovers the outage link begins sending route error (RERR) messages to the source node of the previous decade and intermediates nodes. It repeats this process until route reaches the source node. When the source node receives the RERR, it can renew its discovery mechanism either by sending a new message RREQ or by stopping sending data.

2.2.3 Temporary Ordered Routing Protocol

Temporally ordered routing algorithm (TORA) is a highly adaptive loop-free routing algorithm and is distributed on the basis of the concept of link reversal [12]. It is designed to work in dynamic multi hop network. TORA uses arbitrary height parameter to determine the direction of the relationship between any two nodes for a specific destination. It provides multiple routes for any pair source/destination. As a consequence, it often finds multiple routes for a given destination, but none of them are necessarily the shortest route. To accomplish this, the nodes need to keep neighboring routing information (one hop) contact. Protocol performs three basic functions: creation, maintenance, and erasure the route.

To start the route, the node broadcasts a query packet to its neighbors. This query is re-broadcast through the network until it reaches the destination or an intermediate node that has a route to the destination. Upon receiving the Query packet, the destination nodes sends back an Update packet. On this packet we find attached its height compared to the destination node. As this Update packet is broadcasted throughout the network, it travels from node to node, making them to establish their own height to one higher than the height of the node that sent the Update. This has the effect of creating a series of links from the original sender of the packet query to a node that was born in the first update packet. In case the route becomes unavailable, the node that detects it will start adapting its height to the greatest value compared with the one of its neighbors. After that an Update packet will be sent. If there are no neighbors with limited height in respect to the destination, a new route must be found using the procedure described above.

3 Mutual Authentication and Updating the Authentication Key and the Identities

We propose here a scheme to improve and support mutual authentication and encrypt communication between the nodes in the MANET.

The authentication scheme proposes to solve the security and privacy issues between any two nodes which communicate with each other in the MANET. The scheme includes key searching, mutual authentication and k/ ID updating which can stand most of attacks between the nodes include tracing, impersonate, counterfeiting and eavesdropping. When two nodes want to communicate and exchange data between them, they agree on a secret key or session key between them. Every time a node starts the communication it is called source node or originator and the node that receives the message is the destination.

Variable and the following operators are used

- E_k(M): Conventional encryption result of plaintext m with k as the key.
- D_k(M): Conventional decryption result of cipher text m with k as the key.
- //: Concatenating of two or more messages.
- h (M): One way hash function.
- $\oplus$: Exclusive operation.
- R_s: Random number generated by the source node to verify the destination node.
- R_d: Random number generated by destination node to verify the source node. And we can use it as the key data ciphering after authentication.
- $R_{s,d}$: Random number generated by the source node as the new authentication key for destination node.
- $K_{i,auth}$: The current authentication key and ID of the destination node.
- $K_{i+1,auth}$, metaID_{i+1}: The new authentication key and ID of the destination node generated by the source node.

We suggest a session key between the source and destination node and use it to generate metaID.

We can explain the mutual authentication scheme by these steps (see Fig. 2):

- The source starts the communication, broadcasts the request, generates a random number R_s and sends it to the destination with the request.
- When the destination node receives the message from the source (direct, if it lies in the same range of the source or by intermediate nodes, if it is not in range), the request and random number, the destination generates metaID_i ($\text{metaID}_i = \text{h}(K_{i,auth}, \text{ID})$. After that,

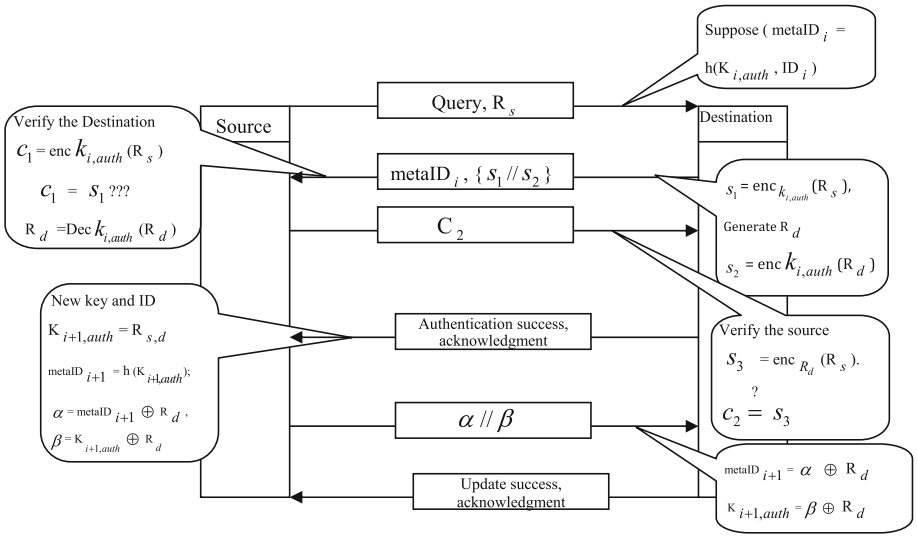

Fig. 2 Challenge and response authentication process and update authentication key

the destination encrypts R_s by $K_{i,auth}$ when it receives R_s from the source, and generates random number R_d which is encrypted by $K_{i,auth}$ to produce s_1 and s_2 respectively:

$$s_1 = \text{enc } K_{i,auth}(R_s), \quad s_2 = \text{enc } K_{i,auth}(R_d)$$

After that, the destination sends $s_1//s_2$ to the source node with metaID_i.

- When the source gets the received $\{s_1//s_2\}$ and metaID_i, it finds the corresponding $K_{i,auth}$ with the received metaID_i as index. After that, the source verifies the destination node by checking $s_1 \stackrel{?}{=} \text{enc } K_{i,auth}(R_s)$. If it equals, the authentication and communication process continues, otherwise, it is disrupted and fails. If the destination is valid the source node decrypts s_2 with $k_{i,auth}$ to get R_d from the destination node. After that, the source node encrypts R_s with R_d to produce c_2, where $c_2 = \text{enc}_{Rd}(R_s)$, and sends it to the destination node.
- When the destination node receives c_2 from the source node, it starts verifying the authentication source node process by checking $c_2 \stackrel{?}{=} \text{enc}_{Rd}(R_s)$. If it equals the authentication process continues, otherwise fails. If the source node is valid, the destination node sends authentication success to the source node (acknowledgement).
- When the source node recognizes that the authentication process succeed, it generates new random number $R_{s,d}$ as the new authentication key $K_{i+1,auth}$ for the present destination node and computes the new corresponding metaID by $\text{metaID}_{i+1} = H(K_{i+1,auth})$; $R_{s,d}$ must be carefully chosen to guarantee that the random number is unique. After that, the source node XoR the new metaID_{i+1}, $K_{i+1,auth}$, pair with R_d respectively and sends them to the destination node α, β where:

$$\alpha = \text{metaID}_{i+1} \oplus R_d, \ \beta = K_{i+1,auth} \oplus R_d$$

- The destination gets new metaID_{i+1}, $K_{i+1,auth}$ after receiving the messages from the source node by XoR α and β respectively by R_d . After that, the destination node updates

the metaID$_i$ and authentication key. Finally, the destination sends acknowledgement to the source node to inform about the update success.

- The source node receives the update success message and replaces the old (metaID$_i$, K$_{i,auth}$) pair with the new (metaID$_{i+1}$, K$_{i+1,auth}$) pair.

The source and destination nodes can use R$_d$ as the secure key to encrypt the data exchanged between them after the successful authentication process.

Example we chose dynamic source Routing Protocol to apply our scheme.

In our protocol, when a node wants to communicate, it initiates route discovery process by generating a RREQ message. Source appends its digital signature (DS) to the message. Neighbors of the source first verify the signature of the source and take the decision accordingly. We added a one way hash function to the RREQ message to maintain the integrity of the message. Therefore, deletion of a node or any kind of modification in route list of RREQ message can be detected. Destination sequence number protocol is added to make the loop free routing and to check the freshness of route control packet.

Assume that S is the source node trying to discover a route to destination D and route from S to D exist via intermediate nodes F, G and X. All the nodes in the network have their own public and private key pair generated by any key management system for mobile ad hoc networks. The nodes which are within range of each other are neighbors. The public key of nodes is known to other nodes in the network.

We still use here L: life time of the package (maximum number of hop), DSS Digital signature of node S, hS Hash value appended by node S to the message.

The operations of our protocol will work as this explanation. A source S initiates route discovery by generating route request (RREQ) message. RREQ contains the address of source and destination nodes, Seq, LREQ, route list of intermediate nodes found on the route from source to destination (initially empty), DSS digital signature of source, and a hash value hS and the random number R$_s$. Life time of a packet refers to maximum number of hops a packet can travel. On each broadcast, life time would be reduced by one automatically. If life time reaches zero, the packet would be discarded. Source produces the hS using one way hash function.

$$\text{hS} = \text{H(S, D, Seq, LREQ)}$$

When a neighbor of S, F, receives the RREQ message with R$_s$, it verifies the signature of source node. If source node is genuine, F checks Seq and compares with Seq stored in its cache. If Seq is less, F discards the packet. Otherwise, it appends its identifier to route list and digital signature DSF to the message and replaces the hS by hF and then rebroadcasts

$$\text{hF} = \text{H(hS, F, LREQ-1), R}_s.$$

Similarly for the next neighbor node, node G verifies the signature of the source and of node F and checks Seq, and then appends its identifier to route list and digital signature DSG to the message, replaces the hF by hG and finally rebroadcasts.

$$\text{hG} = \text{H(hF, G, LREQ-2), R}_s.$$

When the RREQ arrives to the last neighbor node before the destination node, X verifies the signature of the source node, F and G nodes and then appends its identifier to route list and digital signature DSX to the message, replaces hG by hX and the rebroadcasts.

$$\text{hX} = \text{H(hG, X, LREQ-3), R}_s.$$

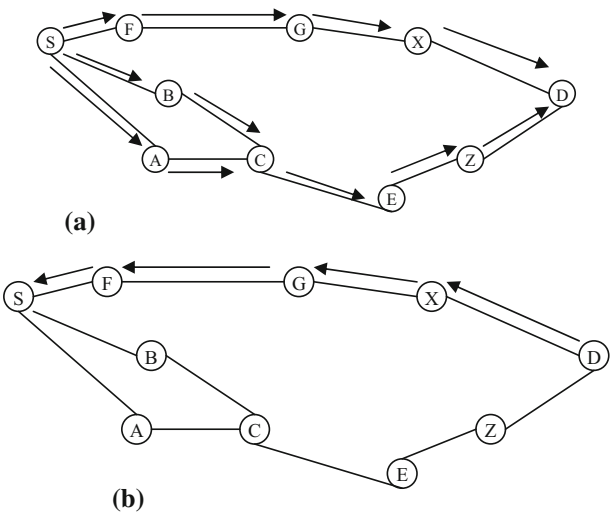

Fig. 3 **a** Route discovery by broadcasting routing request (Rreq), **b** the shortest path for the route replay (Rrep)

Finally, when destination node D receives the RREQ message with source random number R_s, it verifies all the signatures contained in RREQ packet and compares Seq with previously stored Seq in its cache. If source and all the nodes in route list are genuine and the packet is not outdated, the destination node computes (see Fig. 3a):

$$\text{hD} = \text{H((X, LREQ-3, H(G, LREQ-2, H(F, LREQ-1, H(S, D, Seq, LREQ))))}$$

and compares the value of hD with hX. If both values are the same, the message integrity is verified. Otherwise message is discarded. If all the verifications are successful, the destination D creates a route reply (RREP) message and sends it back to the source S via the path obtained by reversing the route list in RREQ packet. Route Reply (RREP) message contains Seq, addresses of source and destination, route list, hD, metaID_i, $\{s_1//s_2\}$, and signature of all the nodes from source to destination. Each intermediate node verifies the signature of destination D and Seq to check the freshness of message. On receiving RREP message at source, S verifies signature of all the nodes in route list and Seq. Source S computes (see Fig. 3b):

$$\text{H} = \text{H ((X, LREQ-3, H (G, LREQ-2, H (F, LREQ-1, H (S, D, Seq, LREQ))))}$$

and compares with hD to check the integrity of route list. If both values are the same, S accepts RREP. Otherwise it discards it. S calculates the values of LREQ-1, LREQ-2 and LREQ-3 on the basis of route list. After successful completion of all verifications, a route from S to D is established.

After that the Source and Destination nodes still communicate with each other to update the authentication key and metaID in the same manner as in our scheme.

4 Security Analysis

In proposed certificate authority in MANET, both new node and group nodes in MANETs authenticate each other mutually at the time of network joining. After successful mutual authentication, nodes can join the network. When two nodes wish to communicate, they also authenticate each other by sending their Digital Signature.

The idea of making On-Demand routing protocols secure represents a real challenge, because, first of all, security attributes and mechanisms have to be understood. Security is viewed as a structure composed from a mixture of processes, procedures and systems. All this components provide access control, confidentiality, integrity, authentication, availability, and non-repudiation.

In our scheme we take care of most kinds of attacks like wormhole attack, impersonation and eavesdropping, by using challenge and response messages between the source and destination nodes. The proposed schemes depend on hash function, random number and authentication key.

Our scheme also takes care of the black hole issue. Generally, one of the most used techniques to ensure the security against this type of attack works as following:

The intermediate nodes are not allowed to send route replies anymore. Those can be generated just by the destination node. In case an intermediate node broadcasts a route reply, the source node transmits a Query in order to check if a path from that intermediate node to the destination node really exists. If such a path is available the intermediate node proves to be trustworthy and can be used by the source node to broadcast data through it. If the node proves to be unreliable, the reply message is ignored. Also, an alarm message is broadcasted into the network and the malicious node is isolated. Now, the source node begins searching for a new route. In this situation, no malicious node can read the message. Why? The password is verified by all the nodes that are forwarding the RREQ. Every node is secure in both directions (from source nodes to destination node) and accomplishes the security demands of the sender.

Furthermore our scheme is suitable for Man in the Middle attack. The Man in the Middle attack is a kind of active attack in which an attacker remains invisible between two nodes like source and destination nodes. Attacker divides the connection in two connections, one between node S and attacker and second between attacker and node D. Two nodes S and D think that they are communicating with each other, while they are communicating with the attacker located between them. Most of the schemes are vulnerable to Man in the Middle attack; where a new joining node sends its public key to a new node in the MANET. In response of request, the node generates a session key and sends it to new joining node, encrypted with new joining node's public key. In this scheme, an attacker may exist between the new joining node and the node of MANET; attacker can capture the public key of the new node and sends its public key to the node in MANET. Then the node in MANET shares the session key with the attacker and the attacker shares session key with the new joining node. But in our proposed mutual authority system, both new node and any node in MANET authenticate each other using challenge-response protocol. Hence, our certificate authority system is not vulnerable to Man in the Middle attack.

5 Comparison Between Our Proposed Scheme and Other Schemes

In MANET, the internal attacks are typically more severe, since the malicious node already belongs to the network. To prevent internal attacks, we need to authenticate the unique

identity of each node. Our proposed scheme provides an efficient way to verify the message authentication and message integrity. The receiver node can authenticate the sender of the message as well as the intermediate nodes using the shared authentication key.

We compared our proposed scheme with secure AODV (SAODV) protocol in the presence of black hole attack [4]. A black hole attack is a kind of denial of service attack in which a malicious node assigns small hop count and high sequence number to the route reply message (RREP) and absorbs all packets by simply dropping them without forwarding them to the destination node. SAODV [10] is implemented as an extension to original AODV protocol. Although SAODV has proposed two alternatives to send RREP message, we used first alternative for implementation: only destination node can send RREP message. We also used hash function to secure hop count and RSA algorithm just for digital signature and also the authentication key and make update to this authentication key and the identities of the nodes to increase the authentication process between the nodes.

In SAODV protocol, both the source node and the intermediate node verify the signature before updating their routing table. A malicious node can impersonate a destination node but cannot generate the signature of destination node. Similarly in proposed method, malicious node does not know the authentication key shared between destination node and others node. The source node or intermediate node discards RREP packets coming from the malicious node and hence, does not establish a route through malicious node.

Time delay of data packet means the difference between the time when the first data packet is received by the destination node and the time when the source node broadcasts a RREQ message. Time delay depends on both mobility and position of nodes. In case of the SAODV protocol and the proposed method, the time delay is more due to delay in establishing particular route as only destination node can send route reply message. Moreover the SAODV protocol has larger time delay compared to our scheme, because SAODV uses asymmetric key cryptography for digital signature and encrypted the data packet between the nodes in the network but in our scheme we use the RSA algorithm just in digital signature and for the data packet transfer between the nodes we use the authentication key, so it requires significant processing time to compute or verify signatures and hashes at each node.

In proposed method, routing uses extra bytes to store hashes and intermediate node addresses. Similarly in SAODV protocol, routing contains extra bytes to store digital signatures and hashes for providing security therefore both methods are the same from this point of view.

Securing MANETs Key Management and Routing [13] they proposed a key management scheme and a secure routing protocol that secures on demand routing protocol such as DSR and AODV. They assume that MANETs is divided into groups having a group leader in each group. Group leader has the responsibility of key management in its group. Proposed key management scheme is a decentralized scheme that does not require any Trusted Third Party (TTP) for key management. Also our proposed scheme and SAODV are decentralized schemes. In proposed key management system, both a new node and group leader authenticate each other mutually before joining the network, like in our scheme a new node and any MANET node authenticate each other mutually before joining the network and before they exchange the data packet. But in SAODV no mutual authentication is used between the nodes. They just depend on the hash chain scheme, while Securing MANETs Key Management and Routing proposed secure routing protocol allows both communicating parties as well as intermediate nodes to authenticate other nodes and maintains message integrity. They also proposed a secure routing protocol especially for On-demand routing protocol. Objective of proposed routing protocol is to authenticate the source and destination and intermediate nodes in route list of route request (RREQ) message and detecting any kind of

Table 1 Comparison between authentication system schemes

Requirement	SAODV protocol	Securing MANETs key management and routing	Mutual authentication and updating the authentication Key in MANETS
Trusted third party	Decentralized scheme	Decentralized scheme	Decentralized scheme
Secure key	Not discuses used public and private key	Used session key	Used authentication key
Updating key	Not implemented	Not implemented	Update authentication key
Updating the identities	Not implemented	Not implemented	Make updating for the metaID
Symmetric or asymmetric key cryptography	Asymmetric key cryptography	Use both symmetric and asymmetric key	Use both symmetric and asymmetric key
Time delay	Larger time delay	Less time delay	Less time delay
Mutual authentication	No mutual authentication	Exist	Exist

modification by a malicious node in RREQ message, providing secure route similarly in our scheme and SAODV. Proposed protocol also allows to intermediate nodes to authenticate its predecessor node, and then rebroadcast the RREQ message. Finally at destination, all nodes are authenticated and checked message integrity and then sends back route reply (RREP) message towards source. We summarize the comparison between the schemes as following in the Table 1.

As shown our proposed protocol provides more security and authentication between nodes, improving also the security of the network because we use authentication key between any two nodes communicate with each other and this authentication key update every exchange process between the source and destination nodes.

6 Conclusion

In this paper, we present the most and important routing protocols: proactive protocol and reactive protocol. Also we propose schemes to increase the security between the nodes by enhancing and improving the authentication and confidentiality between the nodes. The proposed idea uses hash functions and key authentication which is common between any two nodes that communicate with each other, but also digital signatures can be used. We used in our proposal the hash function and random numbers encrypted by authentication key. Our solution expands the security scope them and provides more authentication service between the nodes in MANET.

References

1. Subharthi, P., Pan, J., & Jain, R. (2010). Architectures for the future networks and the next generation Internet. *Computer Communications Journal, 34*(1), 2–42.

2. Stoleru, R., Wu, H., & Chenji, H. (2011). Secure neighbor discovery in mobile ad hoc networks. In *Eighth IEEE international conference on mobile ad-hoc and sensor systems*.
3. Haboub, R., & Ouzzif, M. (2012). Secure and reliable routing in mobile ad hoc networks. *International Journal of Computer Science & Engineering Survey (IJCSES), 3*(1).
4. Secure Ad hoc On-Demand Distan Mobile Networks Laboratory Nokia Research Center FIN-00045 NOKIA GROUP, Finland ce Vector Routing Manel Guerrero Zapata manel.guerrero-zapata@nokia.com
5. Narra, H., Cheng, Y., Çetinkaya, E. K., Rohrer, J. P., & Sterbenz, J. P. G. (2011). Destination-sequenced distance vector (DSDV) routing protocol implementation in ns-3. In *4th international ICST conference on simulation tools and techniques*, ISBN: 978-1-936968-00-8.
6. Chen, T.-W., & Gerla, M. (1998). Global state routing: a new routing scheme for ad-hoc wireless networks. *In Communications, 1998. ICC 98. Conference Record. 1998 IEEE International*.
7. Jacquet, P., Miuhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., & Viennot, L. (2001). Optimized link state routing protocol for ad hoc networks. In *Multi topic conference, 2001. IEEE INMIC. Technology for the 21st century. Proceedings, IEEE international*.
8. Castelluccia, C., & Mutaf, P. (2004). Hash-based dynamic source routing. *LNCS IFIP Networking*, *3042*, 1012–1023.
9. Johnson, D. B., & Maltz, D. A. (1996). *Mobile computing, chapter dynamic source routing in ad hoc wireless networks*. Dordrecht: Kluwer Academic.
10. Mala, C. R., Srinivas, S., Padmashree, S., & Elevarasi, E. (2010) Wireless ad hoc mobile networks. In *National conference on computing communication and technology*, pp. 168–174.
11. Das, S. R., Perkins, C. E., & Royer, E. M. (2000). Performance comparison of two on-demand routing protocols for ad hoc networks. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE* (Vol. 1, pp. 3–12). IEEE.
12. Park, V., & Corson, S. (2001). Temporary-ordered routing algorithm (TORA). Internet draft. draft-ietf-manettora-spec-04.txt.
13. Chauhan, K. K., & Sanger, A. K. S. (2012). Securing mobile ad hoc networks. Key management and routing. *International Journal on AdHoc Networking Systems (IJANS), 2*(2), 65–75.

Ahmad Alomari I was born on the 8th of August 1979 in Irbid, Jordan. I was attracted by the scientific field from a young age, finishing the Al Mazar High School with a Degree in the Scientific Branch and continuing with a Bachelor's Degree in Mathematics from University of Yarmouk—Jordan, College of Science and a High Diploma in Management Information System from the Arab Academy for Banking & Financial Sciences, Faculty of Information Systems & Technology. I am working as a Mathematics and Statistics Teacher for all levels of study and I also have experience in operation research, data base, project management and system analysis teaching. I am currently registered as a PhD student at the University of Bucharest, Faculty of Mathematics and Informatics, Informatics Doctoral School.