Routing Protocol Based Shared and Session Key Exchange Protocol for Wireless Mobile Ad-hoc Network

Md. Golam Kaosar
Victoria University, Australia
golam.kaosar@vu.edu.au

Abstract

Mobile Ad-hoc Network (MANET) is a transitory and infrastructureless network supported by no fixed trusted infrastructure. To achieve security goals like: authentication, integrity, non-repudiation, privacy, a secret key (or session key) is necessary to be shared between the sender and receiver. Because of the nature of MANET, it is unrealistic in many circumstances to implement Certification Authority (CA) concept. Some popular key exchange protocols also have some demerits in case of MANET which are due to mainly the requirement of high computational capability. In this key exchange protocol we propose an algorithm to exchange shared and session key between the sender and destination even during the route creation in various routing protocols.

Key Words: MANET, Key Exchange, MANET routing.

1. Introduction

Mobile node in a MANET operates with limited energy and computational capability due to which load reduction in a node is a common design requirement in MANET. There is no trusted device which could monitor on the security issues in MANET. Nodes operate in cooperative mode and any node can go down anytime it wants or may deny forwarding any packet. At the same time an unknown node can be part of the network anytime and be responsible of forwarding some network packets. Therefore it is easy for malicious node to capture, modify, and generate packets to disrupt MANET. Consequently ensuring security becomes necessary among all other challenging issues, which is not visited as much as it is in case of wired networks.

To ensure privacy, integrity, authenticity etc. some security mechanism must be considered in data communication in MANET. Encryption is one of the techniques to achieve these security parameters. Due to key sharing/exchange problem in private key encryption, public key encryption becomes more popular and widely used. A revolutionary research in public key encryption performed by Diffie-Hellman [1] in 1976 changed the direction of cryptography. Since public key encryption require more computation than private (shared) key encryption, private key encryption would be suitable for MANET because of the less computational capability of mobile devices. On the other hand private key encryption becomes unrealistic in MANET due to the problem of key management [2]. Diffie-Hellman key exchange protocol also may not be suitable for MANET since it requires generating big prime numbers which is quiet a big load for mobile devices. The authors in [4] propose a privacy preserving communication in MANETs where they propose to use different techniques to hide private information of the transmission. The proposed secret key sharing protocol can be utilized in [4] to introduce and enhance the privacy.

In most of the on-demand routing protocols like DSR (Dynamic Source Routing) [5], a RREQ (Route

Request) packet is generated by a sender node whenever it needs to send some packets to a particular node for which it does not know the route. Node cannot start any session unless the path from source to destination is discovered. The proposed algorithm intuitively exchanges a shared secret or session key between the source and destination even during the discovery of the route. Onward that specific pair of nodes would use the shared key for data transmission. Thus it would enhance in ensuring various security parameters in the network.

Organization of the paper is as follows: Section 2 describes some basic of MANET routing protocols. Section 3 and 4 describe the proposed solution and its security analysis respectively. Finally section 5 concludes the paper. This section also provides an implication of future work on this topic.

2. Background

In this section some background information about MANET and its routing protocols are discussed. As it is part of the definition; MANET is an especial kind of network where all the nodes configure themselves. Nodes themselves can act like a router. The topology may also change frequently. Each user of the node has the freedom to move while communicating. One node can take packet from other node and transmit it to its neighboring node. This kind of network works in a standalone fashion. Fig 1 shows a typical ad-hoc network. Unlike wired network in ad-hoc network there are many challenging issues which are very important for the deployment. For example, control message management, dynamic and fast adaptation, speed, power, frequency of updates or network overhead, scalability, security, routing etc. As nodes are mobile and they may disappear anytime, maintaining routing in such network is the most challenging part.

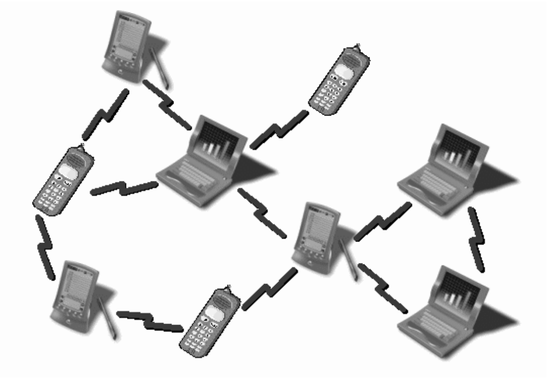

Fig.1: MANET example

There are numerous routing protocols that have been proposed for such kind of network. MANET is classified into three types based on routing protocols which are as follows:

Table Driven Routing Protocols: In Table-driven routing protocols, each node maintains one or more tables containing routing information to every other node in the network. All the nodes update these tables so that a consistent and up-to-date network is maintained. When the network topology changes, the nodes propagate update messages to the entire network. The main disadvantage of proactive routing protocol is that all the nodes in the network always maintain an updated table. Some of the table driven routing protocols are Destination Sequence Distance Vector (DSDV) [6], Wireless Routing Protocol (WRP) [7], Global State Routing (GSR) [8], Fisheye State Routing (FSR) [9] etc.

On-Demand Routing Protocols: These protocols take a lazy approach to routing. In contrast to table-driven routing protocols, all up-to-date routes are not maintained at every node; instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. Unlike Table driven, reactive or on-demand routing protocols do not main an updated table. Some of the on-demand routing protocols are as follows: Ad-hoc On-demand Distance Vector Routing (AODV) [10], Dynamic Source Routing Protocol (DSR) [5], Improved DSR [3] etc.

Hybrid: This is the mixture of both of the above types. Example: Warning Energy Aware Clusterhead Protocol (WEAC) [11]

3. Proposed Solution

In on-demand routing protocol like DSR [5], every node maintains a temporary routing table using which it forwards packets. This routing table is updated whenever an entry expires or a new updated path is discovered. A RREQ packet is generated and broadcasted by the source node whenever it needs to discover a path to a destination. The neighboring nodes re-broadcast the packet and consequently the packet reaches to the destination. A typical RREQ packet anatomy could be <Source_id, Destination_id, path, TTL, other information>. Once the RREQ is reached to the destination it returns a RREP (Route Reply) packet to the source. Thus the source discovers a path.

In this approach we propose some improvements in those routing protocols to enhance the security. In the routing table along with the path to a certain node, there will be another entry to store the secret key to the specific (destination) node. This algorithm suggests different kind of packets to be generated based on different circumstances which depend on presence or absence of route and shared key between the source and destination. If both of them are unavailable then the source will generate and broadcast KRREQ (Key and Route Request) packet which would help develop to create the route as well as the key. If route already exists and the source needs a secret key between itself and the destination, it can only generate a KREQ (Key Request) packet and finally if the route is needed only (in many cases) then only a RREQ (Route Request) packet will be generated and a route will be created only using regular routing algorithm. Furthermore the destination can reply either RREP or KREP (Key Reply) packets based on the request. In brief, this algorithm will work as a regular algorithm as long as there is no need to generate a shared key between the source and destination.

Therefore whenever the source needs to update (or generate a new) secret key for a particular destination, it would initiate either KRREQ or KREQ packet. This will be broadcasted same way like RREQ. The destination may receive multiple copies of RKREQ/KREQ. Unlike the RREQ packet, this time the destination will reply for all the copies along with a simple key generated by itself (different key for different path). Thus the destination will generate keys and send it to the source as many times as it receive the RKREQ/KREQ packet. It will also store the path and key information in a buffer which will be necessary in calculating the secret key later.

On the other hand source node will also receive multiple numbers of RREQ or KREP packets from the destination along with the paths and keys (generated by destination). Of-course the number of received RREP packets may be less than the number actually sent by the destination.

The flow of key generation and exchange of the protocol is depicted in the fig. 2.

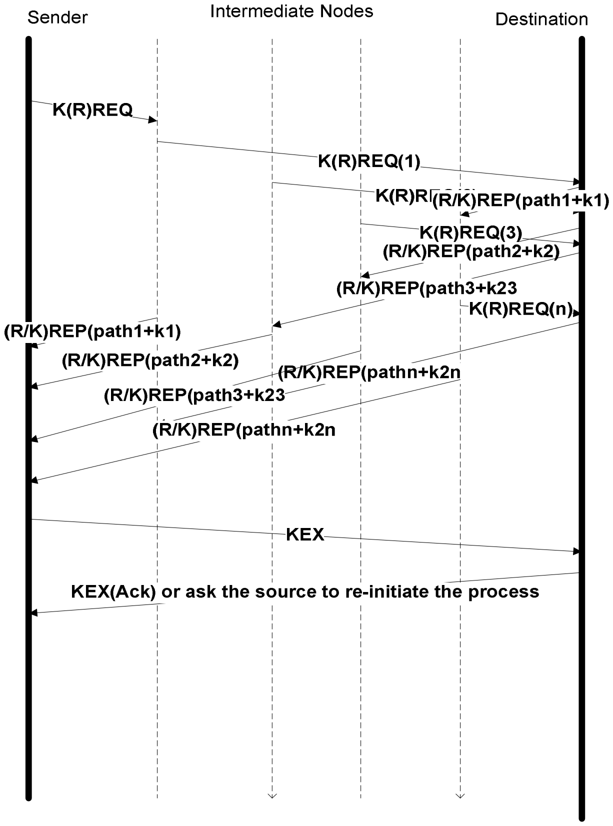

Fig.2: Key generation and exchange steps.

Source		Destination	
Path	Key	Path	Key
P_1	K_1	p_1	k_1
P_2	K_2	p_2	k_2
P_3	K_3	p_3	k_3
…	…	…	…
P_N	K_N	p_n	k_n

Table 1: Typical entries of their buffers

Next the source will combine all paths and keys to generate a secret key. That is:

$$K_{SD} = \int (P_1, P_2, P_3, \ldots\ldots P_N; K_1, K_2, K_3, \ldots\ldots K_{N)}$$

$$E_{ID} = E_{KSD}(\text{Source ID})$$

Where,

P_i →is the path from source to destination found in i^{th} RREP packet.

K_i →is the key provided by the destination with ith RREP packet.

∫ → Cryptographic key generation function.

E_{ID} → Encryption of Source_ID using K_{SD}.

Then the source would find the shortest path and update its routing table and send another packet KEX (Key Exchange) anatomy of which can be as <Source_ID, Destination_ID, path, TTL, EID, other information>.

Key discovery in destination: Destination node has the record of all RREP packets which consists of set of paths p_1, p_2, p_3……. p_n and keys k_1, k_2, k_3 …….. k_n generated by itself. Here obviously n>=N since all the RREP packets sent by the destination may not reach to the source.

Destination will perform following operations:

$$K_{SDi} = \int (p_1, p_2, p_3, \ldots\ldots p_n; k_1, k_2, k_3, \ldots\ldots k_{n)}$$

$$D_{IDi} = D_{KSDi}(E_{ID})$$

Where,

p_i →is the path from source to destination sent in ith (K/R)REP packet.

k_i →is the key provided by the destination sent in ith (K/R)REP packet.

∫ → Cryptographic key generation function.

K_{SDi} → Key generated in ith iteration.

D_{IDi} → Decryption of E_{ID} using the key K_{SDi} (In successful iteration this will be equal to the destination_ID).

Flow diagram of the key discovery process is illustrated in Fig. 3:

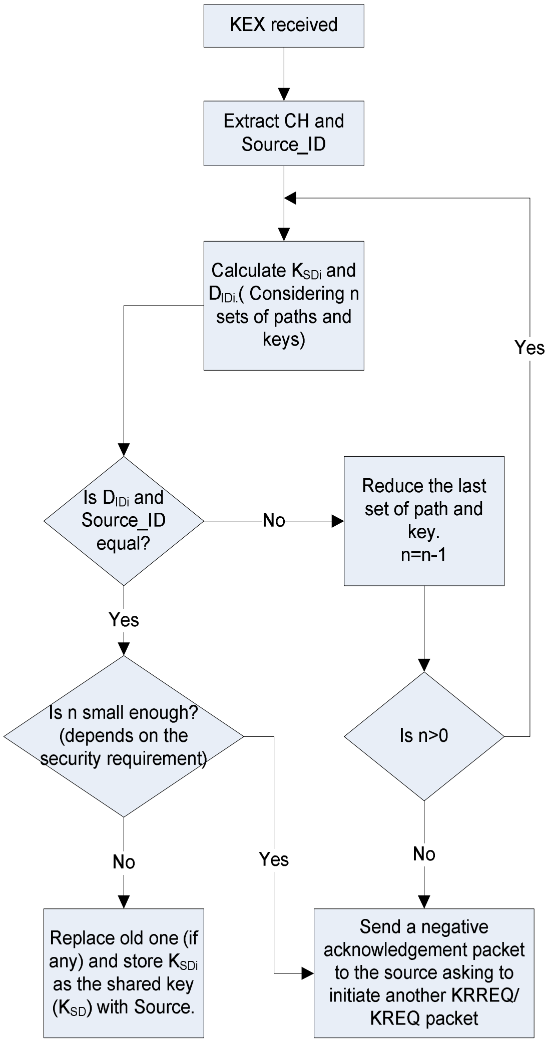
KEX received
Extract CH and Source_ID
Calculate K_{SDi} and D_{IDi}(Considering n sets of paths and keys)
Yes
Is D_{IDi} and Source_ID equal?
No
Reduce the last set of path and key. n=n-1
Yes
Is n small enough? (depends on the security requirement)
Is n>0
No
Yes
No
Replace old one (if any) and store K_{SDi} as the shared key (K_{SD}) with Source.
Send a negative acknowledgement packet to the source asking to initiate another KRREQ/ KREQ packet

Fig.3: Flowchart of key discovery by the destination node

Considerations: The larger the network is the stronger key the algorithm will generate. If there is only single path between the source and destination or a certain node is common in all the paths, the key will be the weakest one. In such case the source will either use this weak key or wait sometime before resending the request for KRREQ/KREQ packet. In case of self mobile network, the node may change its position so that there can be multiple paths between itself and the destination. Once the key is shared, it can be used for long period of time agreed by both party.

4. Security Analysis

The intermediate keys generated and sent by the destination are delivered to the source in different paths therefore there is low probability that a single intermediate node will be able to know all keys. Therefore the whole set of keys are only known to the source and the destination. Upon receiving the number of sets of paths and keys, the source will generate a shared key. Later on during key exchange, the source will encrypt its ID (Source_ID) using the newly generated key which will be forwarded to the destination. From this information no intermediate node could discover the secret key easily unless they have all the sets of paths and keys. Furthermore to make the key stronger, the source can discard the key and re-initiate the procedure if any of the two following circumstances occur; First: if there is any node common in all the paths, secondly: if number of sets of paths and keys are too small.

In case of larger network the proposed algorithm would generate stronger keys since possibility if getting multiple paths is high and possibility of getting single node in all paths will be low. This algorithm is also much suitable and would generate stronger keys in a network where nodes can move independently. In which case the node can change its location to change the set of neighbors and generate new keys until it considers a shared key is strong enough.

5. Conclusion and Future Work

This protocol has very less overhead since key can be shared during regular route discovery. Shared key encryption is very simple and fast which would make MANET data exchange faster. If the key is suspected to be compromised, a new key can be discovered. No intermediate node can predict the key unless most of the intermediate nodes are compromised.

Main weakness of the protocol is: if the number of paths are small and one or more nodes are common to all the paths then that particular node(s) can calculate the key. But the receiving node can determine such circumstance and discard such key and generate a new one. Moreover if the nodes have mobility, they can change their geographical location to make the key stronger.

The larger the network is the stronger the key will be. It is anticipated that farther experiment and implementation would establish that the proposed protocol would generate and exchange shared key with less effort which is one of the most essential features in MANET.

References

[1] Diffie W and Hellman M, “New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[2] Muto K.; Kikuchi H.; Arimichi H. “A proposal for and evaluation of secure key management in service operation schemes”, Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP, 10-14 April 2000 Page(s):683 – 696.

[3] M. G. Kaosar, A. S. H. Mahmoud, T. R. Sheltami, "Performance Improvement of Dynamic Source Routing Protocol Considering the Mobility Effect of Nodes in Cache Management.", The third IEEE and IFIP International Conference on wireless and Optical Communications Networks

(WOCN 2006), April 11-13, 2006, Bangalore India. IEEE Catalog No: 06EX1360C, ISBN: 1-4244-0340-5.

[4] Heesook C.; Patrick M.; Thomas F.; "Privacy Preserving Communication in MANETs", Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on 18-21 June 2007 Page(s):233 – 242.

[5] D. B. Johnson, D. A. Maltz "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, Kulwer, 1996, pp. 152-81.

[6] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Comp. Comm. Rev., Oct. 1994, pp.234-244.

[7] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.

[8] Tsu-Wei Chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proc. IEEE ICC©98, 5 pages.

[9] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad-hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.

[10] VD Park and MS Corson "A highly adaptive distributed routing algorithm for mobile wireless networks", Proc. INFOCOM©97, Apr. 1997, 9 pages.

[11] T. R. Sheltami, H. T. Mouftah, .An Efficient Energy Aware Clusterhead Formation Infrastructure Protocol for MANETs. Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC.03) 1530-1346/03, 03 IEEE.