Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Issues In Mobile Ad-hoc Network With Implication of Key Management: A Review

Shilpa Bansal[1],
[1] M-Tech.Scholar RPIIT TECHNICAL CAMPUS, KARNAL (INDIA)

Dinesh Kumar[2]
[2]Asstt. Professor, RPIIT TECHNICAL CAMPUS, KARNAL (INDIA)

Abstract:-Mobile ad-hoc network is a special kind of wireless network. Security in mobile ad-hoc network is difficult to achieve because of vulnerability of wireless links. This paper will work on nodes to provide security over transmission with finding the shortest path over entire network through Bellman-Ford algorithm and using security providing algorithms that is Diffie-Hellman and General Diffie-Hellman.

Keywords: Bellman-ford, DH, GDH, MANET.

I. Introduction

These days with the rapid proliferation of wireless lightweight devices such as laptops, wireless telephones and particularly mobile ad-hoc networking have become apparent. A mobile ad-hoc network (MANET) is a self-configuration wireless ad-hoc network of mobile nodes. The union of connection of nodes is an arbitrary topology. A mobile ad-hoc network is a temporary infrastructureless network, formed by a set of wireless mobile hosts that dynamically establish their own network on the fly, without relying on any central administration [4]. A MANET is a communication network characterized by the absence of any fixed infrastructure. It is formed spontaneously with the participating nodes without any preplanning [6].

A MANET organization depends upon the location of the nodes, their connectivity, their service discovery capability, and their ability to search and route messages using the nearest node or nearby nodes. MANET is introduced to overcome the deficiencies facing in fixed infrastructure.

The problems with fixed infrastructure is that

(1) It is not suitable in operation like disaster relief.

(2) If a wireless device or mobile devices moves out of range of access-point, base station, or gateway then it is unable to communicate through the network. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication and automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network [5].

Mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network [4], including:

- ***Peer-to-Peer***:-Communication between two nodes which are within one hop. Network traffic (Bps) is usually consistent.
- ***Remote-to-Remote***:-Communication between two nodes beyond a single hop but which maintain a stable route between them. This may be the result of several nodes staying within communication range of each other in a single area or possibly moving as a group. The traffic is similar to standard network traffic.
- ***Dynamic Traffic*:-**This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.

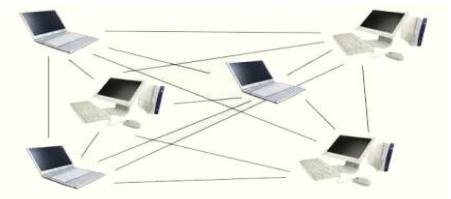

Fig.1 Example of Ad-hoc network

A. ***Security challenges:-*** Wireless mobile ad hoc nature of MANET brings new security challenges to network design. Mobile adhoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks or infrastructure-based wireless networks.

- ***Confidentiality*** ensures that classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.
- ***Integrity*** guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.
- ***Availability*** implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.
- ***Authenticity*** is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.
- ***Non-Repudiation*** ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

B. MANET Features:-

- ***Autonomous terminal***. In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
- ***Distributed operation***. Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.
- ***Multihop routing*****.** Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate Nodes.
- ***Dynamic network topology***. Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network(e.g. Internet).
  (a) Infrastructure-based wireless network
  (b) Ad hoc wireless network
- ***Fluctuating link capacity*****.** The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.
- ***Light-weight terminals***. In most cases, the MANET nodes are mobile devices with less CPU processing capability,Small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

C. MANET Applications:-

- ***Military battlefield***: - Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.
- ***Commercial sector***: - Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

- ***Local level*:-** Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium,boat and small aircraft,Mobile ad hoc communications will have many applications.
- ***Personal Area Network (PAN)*:-**Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

II. Bellman-Ford Algorithm

This is the simplest algorithm which work on the network to find the shortest path across the entire network. The Bellman–Ford algorithm computes single-source shortest paths in a weighted digraph. For graphs with only non-negative edge weights, the faster Dijkstra's algorithm also solves the problem. Thus, Bellman–Ford is used primarily for graphs with negative edge weights. The algorithm is named after its developers **Richard Bellman**and **Lester Ford,Jr**. Negative edge weights are found in various applications of graphs, hence the usefulness of this algorithm However, if a graph contains a "negative cycle", i.e., a cycle whose edges sum to a negative value, then walks of arbitrarily low weight can be constructed by repeatedly following the cycle, so there may not be a shortest path. In such a case, the Bellman-Ford algorithm can detect negative cycles and report their existence, but it cannot produce a correct "shortest path" answer if a negative cycle is reachable from the source[3].
Bellman-Ford algorithm is designed for directedgraphs. If *G* is undirected, replace every edge (u,v) with two directed edges (u,v) and (v,u), both with weight w(u,v).

Time Complexity:-

Time = $O(|V|\,|E|)$.

III. Diffie – Hellman Algorithm

A cryptographic key exchange method developed by **Whitfield Diffie** and **Martin Hellman** in **1976**. Also known as the **"Diffie-Hellman-Merkle"** method and **"exponential key agreement,"** it enables parties at both ends to derive a shared, secret key without ever sending it to each other.

Diffie Hellman key exchange algorithm uses asymmetric key principles for the distribution of symmetric keys to both parties in a communication network. Key distribution is an important aspect of conventional algorithm and the entire safety is dependent on the distribution of key using secured channel. Diffie Hellman utilizes the public& private key of asymmetric key cryptography to exchange the secret key.
Primitive root of a prime number 'p' as one whose powers generate all the integers from 1 to p-1, i.e. if 'a' is the primitive root of a prime no 'p', then,

The steps for Diffie Hellman key exchange algorithm are:

Step 1: GLOBAL PUBLIC ELEMENTS
Select any prime no: 'q'Calculate the Primitive root of q: 'a' such that a<q.

Step 2: ASYMMETRIC KEYGENERATION BY USER 'A'Select a random number as the private key X_A where $X_A< q$.
Calculate the public key Y_A where $Y_A = a^{X}{}_A \bmod q$.

Step 3: KEY GENERATION BY USER 'B'
Select a random number as the private key X_B where $X_B< q$
Calculate the public key Y_B where $Y_B = a^{X}{}_B \bmod q$.

Step 4 : Exchange the values of public key between A & B

Step 5: SYMMETRIC KEY (K) GENERATION BY USER 'A'$K= Y_B{}^{X}{}_A \bmod q$

Step 6: SYMMETRIC KEY (K) GENERATION BY USER 'B'$K= Y_A{}^{X}{}_B \bmod q$.

A. Example of Diffie-hellman key Exchange:-

***1). Discrete logarithmic problem*:** Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network

Alice				**Bob**		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
A	p, g		p,g⟶			B
A	p, g, A	$g^a \bmod p = A$	A⟶		p, g	B
A	p, g, A		⟵B	$g^b \bmod p = B$	p, g, A, B	B
a, **s**	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**

Alice and Bob agree to use a prime number p=23 and base g=5.

1. Alice chooses a secret integer $\boldsymbol{a}$=**6**, then sends Bob A = $g^a \bmod p$
   - A = $5^6 \bmod 23$
   - A = **15,625** mod 23
   - A = 8
2. Bob chooses a secret integer $\boldsymbol{b}$=**15**, then sends Alice B = $g^b \bmod p$
   - B = $5^{15} \bmod 23$
   - B = **30,517,578,125** mod 23
   - B = 19
3. Alice computes **s** = $B^a \bmod p$
   - **s** = $19^6 \bmod 23$
   - **s** = **47,045,881** mod 23
   - **s** = **2**
4. Bob computes **s** = $A^b \bmod p$
   - **s** = $8^{15} \bmod 23$
   - **s** = **35,184,372,088,832** mod 23
   - **s** = **2**
5. Alice and Bob now share a secret: **s** = **2**. This is because 6*15 is the same as 15*6. So somebody who had known both these private integers might also have calculated s as follows:
   - **s** = $5^{6*15} \bmod 23$
   - **s** = $5^{15*6} \bmod 23$
   - **s** = $5^{90} \bmod 23$
   - **s**=8**07,793,566,946,316,088,741,610,050,849,573,099,185,363,389,551,639,556,884,765,625** mod 23
   - **s** = **2**

Simplified form

- Let **s** = shared secret key. **s** = **2**
- Let g = public base. g = 5
- Let p = public (prime) number. p = 23
- Let **a** = Alice's private key. **a** = **6**
- Let A = Alice's public key. A = $g^{\mathbf{a}} \bmod p = 8$
- Let **b** = Bob's private key. **b** = **15**
- Let B = Bob's public key. B = $g^{\mathbf{b}} \bmod p = 19$

IV. General Diffie-Hellman Algorithm

A .An Overview:-

Steiner *et al*. [2] proposed an n-party generalization of the basic two-party DH protocol the new protocol consists of n rounds, allowing n nodes to establish a common key. In the first $n - 1$ rounds contributions are collected from each node. In the first round, $M1$ generates $r1$ and computes a$r1$, which it sends to $M2$. In the second step $M2$ generates $r2$, computes a$r2$ and sends it to $M3$, along with a$r1$ and a$r1 \times r2$. This latter sends to $M4$ (after making the required computations) the third-round partial factors, i.e., a$r1 \times r2$, a$r1 \times r3$,a$r2 \times r3$, as well as the third-round partial key a$r1 \times r2 \times r3$. This process continues for each Mi (i

<n). Upon the (n – 1)th round, the collector node *Mn* receives the (n – 1)th round partial factors, and the (n – 1)th round partial key, then it generates its random number and computes the final key *K*.4 In the last round, node *Mn* sends each *Mi* the appropriate (n)th round partial factor, i.e., Consequently, each node uses its random number to compute the common key *K*. Note that partial factors are used to avoid sending the final resulted key during the last round. Also note that the (n – 1) th round requires n – 1 operations (sending the partial factor to each node), which makes the computational complexity of the solution= (2 × (n – 1))[4].Even though it uses a collector, this solution is contributory, since each node contributes to the key computation with the random number it generates.

B. Computational complexities=(2*(n-1))

V. Conclusion and Future work

This article will work to provide the security over transmission with n number of nodes. If the data transmission is done upon two nodes then this procedure is best for secure transmission but this will not work properly if the number of nodes are more than two because it will cause wastage of time and money. This procedure will create the overhead on the network as it needs to provide the security on each and every node. And we can consider it as our future work to provide the procedures, which will overcome drawbacks of wastage of time and complexities.

References

[1] Ad Hoc Networking Extended Research Project. Online Project. http://triton.cc.gatech.edu/ubicomp/505.

[2] M. Steiner, G. Tsudik, and M. Waidner, "Diffie Hellman Key Distribution Extended to Group Communication," ACM Conf. Comp. and Commun. Security, 1996, pp. 31–37.

[3] Cormen, Thomas H;Leiserson, Charles E, Rivest, Ronald L.Introduction to Algorithms. MIT Press and McGraw-Hill, Second Edition.MIT Press and McGraw-Hill,2001.Section 24.1: The Bellman-Ford algorithm,pp. 588-592.

[4] Djamel Djenouri and Lyes Khellari,Cerist Center of Research,Algiers Nadjib Badache, "A survey of security issues in Mobile Ad-Hoc network and Sensor network" IEEE communication Surveys and Tutorials. Fourth Quarter 2005.

[5]. Aboba , D. Thaler , L. Esibov, The Link Local Multicast Name Resolution (LLMNR), Microsoft Corporation , January 2007, RFC 4795.

[6] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor , "Group Key Management in MANETs" International Journal of Network Security, Vol.6, No.1, pp.67-79, Jan 2008.

