International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
Volume 2 Issue 1 2011

REVIEW OF SECURED ROUTING FOR WIRELESS AD HOC NETWORK

Satish Kumar Garg
Govt. PG College Jind (Haryana), India,
sat.phy@gmail.com

Abstract

An ad hoc Network provides a infrastructure less communication over a shared Wireless Channel and operates without the use of existing network in which all mobile nodes can communicate with a centralized structure. This becomes the main reason, for this technology to be more vulnerable to security attack and security threats. Such attack includes passive eavesdropping over the wireless channel, denial of service attacks by malicious nodes and attack from promised node or stolen devices. In this paper, we present review on the security issues of existing routing protocols in an ad hoc network environment and try to identify some source of threats to routing protocols. Aim is to make existing environment more secure from all type of security threats and some of vulnerable attacks. This study will help to Ad hoc networks researchers for developing secured routing.

1.0 Introduction:

Ad hoc network are new are new paradigm of wireless communication the nodes. In ad hoc network, there is no fixed infrastructure such as base station or mobile switching centers. As ad hoc networking where potential mobile user arrive within the common perimeter of radio link and participate in setting up the topology for communication. Nodes with in ad hoc are mobile and they communicate with each other within radio range through direct wireless links or multihop routing. Thus in such a environment it became much necessary for the mobile host to enlist the aid for other hosts is forwarding a packet to its destination, due to limited range of each mobile host wireless communication. [1,10,11] The main application for the ad hoc networking is military tactical communication known as Packet Radio Networking for example, a class of students may need to interact during a lecture, friends, or business associates may run into each other in an airport terminal and wish it share files or important information, or a group of emergency rescue workers may need to be quickly deployed after a earthquake or flood. In such a case, a collection of mobile hosts with wireless network interface may form a temporary network without the aid of any established infrastructure or centralized administration. Thus it is obvious that lack of infrastructural support and susceptible wireless link attack there are two types of attacks toward security protocols.

External attacks: It can be active or passive. Passive are unauthorized interrurting the routing packets and active is from outside sources to degrade or damage message flow between nodes.

Internal attacks: a compromised node is categorized internal attack. This is most serve threat for ad hoc networks. This may broadcast wrong routing information to other nodes.

The inheritance feature of wireless networks poses opportunities for attack from passive eavesdropping to active impersonation, message distortion. As is often the case, proper security was not built in at beginning.

Rest of the paper is organized as : section 2 describes requirements for wireless network security, section 3 takes a look at pitfalls in security aspects , section 4 is description of existing work, section 5 gives a proposed plan , section 6 concludes the study with references.

2.0 Requirements for the Wireless network security:

In this, we are highlightened; the security properties required by ad hoc network security routing, [1, 4] some are as follows.

Availability:

It ensures that the survivalablity of network services despite denial of service attacks. A denial service attack could be launched at any layer of ad hoc network on the network layers; an adversary could disrupt the routing protocols and disconnect the network.

Data Confidentiality:

It ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain case, because the information might be vulnerable for enemies to identify and to locate their target in a battlefield. Hence, Ad hoc Network should not leak readings to some other neighboring networks.

Data Authentication:

It enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade anode, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes. Hence data authentication allow a receiver to verify that data really was sent by the claimed sender, the receiver believe that the message was correct and by correct sender.

Data integrity:

It ensures that the message being transferred is never corrupted. The adversary does not alter the received data in transit and this one is stronger property. i.e. protecting the node from malicious altered message hence the recipient must be sure that the source is genuine and data is not modified by malicious or unauthentic user.

Data freshness:

Data freshness implies that the data is recent and it ensure that no adversary replayed old message, there are two type of data freshness one is weak freshness which provide partial message ordering, but comes no delay information and strong freshness, which provide a total order as a request-replace pair, and allow for delay estimation, weak freshness is required by measurements, while strong freshness is useful for time synchronization with in network.

Non-repudiation:

It ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B compromised

There are other security goals (e.g. authentication) that are of concern to certain applications, that to be achieved for any secure routing in ad hoc network.

3.0 Security pitfalls in wireless Networks:

As wireless networks have no predefined structure and, services are created and configured on the fly, so due to these reasons the network security is inherently weak. [1, 2, 6, 11, 9]

The nature of attacks vary greatly from one set of circumstances to another. In general, there is flow of information from a source to a destination. We have listed below the generic types of attack that might be encountered. They have also been pictorially depicted.

_ **Interruption:** An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.

_ **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Examples include wiretapping to capture data in a network and the illicit copying of files or programs.

_ **Modification:** An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.

_ **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

A categorization of these attacks in terms of passive and active attacks is shown in Fig 1.

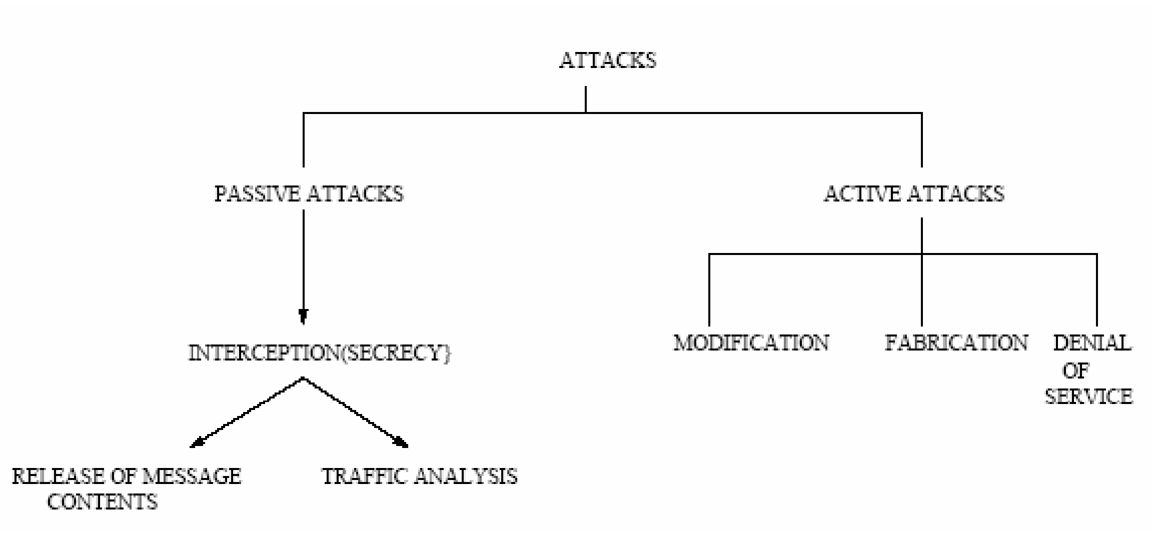

Figure 1

Active Attacks

These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.

1. *Masquerade:* This takes place one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attacks.

2. *Replay:* This involves passive capture of data units and its subsequent retransmission to produce an unauthorized effect.

3. *Modification of Messages:* This simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered.

4. *Denial of Service:* This prevents the normal use or management of communication facilities. One form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance.

It is quite difficult to prevent active attacks absolutely, as this would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them. because the detection has a deterrent effect, it may also contribute to prevention.

4.0 Related work:

In this paper, we review all related work that deal with security issues in existing ad hoc wireless network. Patel and Crowcroft are focused on security protocols for the mobile user devices [8] but as they used the asymmetric cryptography, is too expensive for the wireless environment. None of the system provides mechanism to defeat mobile adversaries and to achieve network more secure, and more data authentication broadcasting.

To achieve the [4,6,8,1] security requirements in ad hoc Wireless Network the following building blocks SNEP (security network encryption protocol) provides and µTESLA (the "micro" version of the Timed, Efficient, Streaming, Loss-tolerance Authentication Protocol), providing authenticated streaming broadcast, so these two designed protocols are very useful for making the existing system.

4.1 SNEP:

This provides a numbers of unique advantages. SNEPS [4] offers the following nice properties.

Semantic Security:

Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats with in the lifetime of the code.

Data Authentication:

If the MAC verifies correctly, a receivers can be assured that the massage originated from the claimed senders.

Weak freshness:

If the message verified correctly, a receiver knows that the message must have been sent after the previous message it received correctly hence this enforces a message ordering and yields a weak freshness

4.2 µTESLA:

Authenticated broadcast [7, 10, 15 12, 11, 14, 13] symmetric mechanism for safe sending data so that data could be sent properly, otherwise any compromised receiver could forge message from sender. Unfortunately, asymmetric cryptographic mechanisms have high computation, communication, and storage overhead, which make their usage on resource-constrained devices impractical. µTESLA overcomes these problems by introducing asymmetry through a delayed disclosure of symmetric keys, which result in an efficient broadcasting authentication scheme.

Proposed TESLA updated as µTESLA as it was mainly designed for the sensor network only so it was not fit for the wireless network for the following reasons

TESLA authenticates the initial packet with a digital signature for nodes and it uses the mechanism that is not symmetric.

Disclosing a key in each packet require too much energy for sending and receiving.

µTESLA [4] overcomes these problems by introducing asymmetric through a delayed disclosure of symmetric key, which is result in an authenticated broadcasting. Currently proposal for authenticated broadcast are impractical as firstly all proposals are relay on asymmetric digital signature for authentication which are impractical for multiple reasons as they require more signature with high communication overhead for to create and verifications signatures but recently proposed µTESLA protocol provides efficient authenticated broadcast. µTESLA requires that the base station and nodes are loosely time synchronized, each nodes knows an upper bound on the maximum synchronization error. To send an authenticated packet, the base station simply computes a MAC on the packet with a key that is secreting at that point in time. When a node gets a packet, it can verify that the corresponding MAC key was not yet disclosed by the station since a receiving node is assured that only the base station knows the MAC key, the receiving node is assured that no adversary could have altered the packet in transit. The node stores the packet in buffer. At the time of key disclosure, the base station broadcast the verification key to all receivers. When a node receives the disclosed key, it can easily verify the correctness of the key. If the key is correct, the node can now use it to authenticate the packet stored in buffer.

5.0 Proposed plan:

The study is limited in many ways in ad hoc network. Some of the issues that have not been properly addressed, there are many additional issues which have not been addressed for the proper security of ad hoc network. We have proposed the solution for authenticated broadcasting such as data authentication, data confidentiality, data integrity, data freshness, non-repudiation; these are security goal for any application to be achieved. For our security measures, we proposed to implement µTESLA due to its distributed nature, if these are implemented in ad hoc network the routing protocol will be more secure as these provides semantic security some other facility for securing ad hoc network. Some of the measures that can be incorporated are:

1. **Virtual Private Networks (VPN)** This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors as password, Fingerprints and a security Token. Using two factors is desirable and using all three is most secured. VPN only support IP suite so it cannot be solution for all environments.

2. **Encryption:** Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Ciphertext (or Cipher). The process of changing plaintext into ciphertext is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA) These are based on key based algorithms. There is one popular key algorithm as Digital signature algorithm. In Digital signature, Signer encrypts the message with key, this is sent to recipient, the message is then decrypted with sender's public key. In case of ad hoc networks this may not be the best method as it uses a lot of space and is also slow.

3. **One Way Hash Function**: There is another algorithm called One way hash Function: it is like checksum of a block of text and is secure in that it is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces a affixed size tag as output. This algorithm can be combined with encryption to provide an efficient and effective digital signature.

4. **Digital Signature**: External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signatures and one way functions can be applied [12]. Permian[18] used

complex robustness to protect routing data from compromised nodes. It is ability to continue correct operation in presence of arbitrary nodes with complex failures.

6.0 Conclusion:

In this paper, security relevant issues with in ad hoc networks are identified and their significant usage advantage on the well defined security architecture where security aspects like confidentiality, integrity and availability are addressed properly. Several issues have been suggested to achieve gal of security . There are some aspects which we are trying to cover as Overhead caused by adding security parameters. Speed of data transmission , which will be affected due to added size. Also medium of transmission is to be taken care of , which can be denser or sparse. The problems of information through covert channels is also not addressed in this paper . we are trying to incorporate the security parameter as “key encryption” to existing routing protocols and see the effect of it. The major issue is overhead and speed of data transmission.

7.0 REFERENCES:

[1] Zhou and Z.J.Haas, “Secure Ad hoc Networks”, IEEE Networks,13(6):24-30, Nov/Dec 1999

[2] 3GPP,: 3G Security: Security Architecture”, 3GPP TS 33.102 V3.6.0, Oct.2000

[3] Preetida,”Security with in Ad hoc Networks” Position paper, PAMPS Workshop, Sept 2002, London

[4] Adrian Perrig, Robert Szewczyk, J.D. Tyagar, “SPINS: Security Protocols for sensor Network “, Department of Electrical and Computer Sciences, University of California

[5] S.Murphy and J.J.Garcia-Luna-Aceve.,” An efficient routing algorithm for mobile wireless network.”, MONET, I(12):183-197, Oct1996

[6] B.Kumar. ,“Integration of security in network routing protocols” , SIGSAC reviews 11(2):18-25, 1993.

[7] David W. Carma, Peter S. Kruus, and Brian J Matt, “constraints and approaches for sensor network security”, NAI Labs Technical Report #00-010, September 2000

[8] Bhrat Patel and Jon crowcroft, ”Ticket based service access for mobile user.” In Third annual international conference on Mobile ad hoc networking, Hungary, September 1997.

[9] D. Johnson and D.A. Maltz and J. Broch,” The dynamic source routing protocol for mobile as hoc networks (internet-draft).”, In Mobile Ad-hoc network (MANET) Wprlemg Group, IETF, PVTPNER 1999.

[10] Z.j. Haaas and M. Perlman., “ The zoone routing protocol (ZRP) for ad hoc networks “,(Internet-Draft).1998

[11] D.B. Johnson and D.A. Maltz.,” Dynamic source rerouting in ad-hoc wireless network.”, In Mobil Computing,1996

[12] Young-Bae Ko and Nitin Vaidya., “Location-aided routing (LAR) in mobile ad hoc networks.” In Proceedings of the Fourth International Conference on Mobil Computing and Networking (Mobicom’98, October 1998

[13] V.D. Park and M.S. Corson., “A highly adaptable distributed routing algorithm for mobile wireless networks.” In IEEE INFOCOMM’97,1997

[14] C.E.Perkins and E.M. Royor,” Ad hoc on-demand distance vector routing.”, In IEEE WMCSA’99,February 1999

[15] C.E.Perkins and P.Bhagwat,” Highly dynamic destination sequence distance-vector routing (DSDV) For mobile computing.” In ACM SIGCOMM Symposium on Communication, Architectures and Application, 1994.

[16] K.S.J.Pister, J.M.Kahn and B.E. Boser. ,”Smart dust: Wireless networks of millimeter-scale sensor nodes”, 1999