ISSN No. 0976-5697

Volume 5, No. 3, March-April 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Review of Hybridized Routing and Tolerant Security Mechanism for Wireless Ad hoc Networks

Gavendra Sahu*
M.Tech, Computer science & Engineering Department
Rungta College of Engineering and Technology
Kohka Kurud Road, Bhilai, India
gebu_131184@yahoo.co.in

Neelabh Sao
Reader, Computer Science & Engineering Department
Rungta College of Engineering and Technology
Kohka Kurud Road, Bhilai, India
neelabhsao@gmail.com

Abstract: Ad hoc Networks are an emerging area of mobile computing. There are various challenges that are faced in the Ad hoc environment. These are mostly due to the resource poorness of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. Ad hoc Networks therefore throw up new requirements and problems in all areas of networking. The solutions for conventional networks are usually not sufficient to provide efficient Ad hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. In this paper we attempt to analyze the demands of Ad-hoc environment. We focus on two areas of Ad hoc Networks, Ad hoc routing, and intrusion detection. The key issues concerning these areas have been addressed here. We have tried to compile solutions to these problems that have been active areas of research.

Keywords: Ad hoc networks; AODV; DSR; Routing; Protocols

I. INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts. No fixed infrastructure such as base stations as mobile switching. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. Ad hoc Networks is defined as a collection of mobile hosts forming a temporary network without the aid of any centralized administration or standard support services. In other words an Ad hoc Network [1] is a network whose is on the basis of temporary. An Ad hoc or spontaneous network is a local area network or any other network, especially one with wireless or temporary plug in connections, in which some of the network devices are the part of the network only for the duration of a communication period, whereas in the case of portable mobile devices it is part of the network when in some close proximity to the rest of the network.

A. *Security Goals:*

The basic factors in security is as follows [2] which includes

- ***a.*** ***Availability:*** Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.
- ***b.*** ***Confidentiality:*** Ensures certain information is never disclosed to unauthorized entities.
- ***c.*** ***Integrity:*** Message being transmitted is never corrupted.
- ***d.*** ***Authentication:*** Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.
- ***e.*** ***Non-repudiation*** ensures that the origin of a message cannot deny having sent the message.

B. *Challenges:*

Use of wireless links renders an Ad hoc Network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion [3]. Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc thus violating availability, integrity, authentication and non-repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. For high survivability Ad hoc Networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad hoc Network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the fly (dynamic) and not static and should be scalable.

C. *Secure Routing:*

The contemporary routing protocols for Ad hoc Networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. No single standard protocol [4]. Capture common security threats and provide guidelines to secure routing protocol. Routers exchange network topology informally in order to establish routes between nodes another potential target for malicious attackers who intend to bring down the network. External attackers injecting erroneous routing info, replaying old routing info or distorting routing info in order to partition a network or overloading a network with retransmissions and inefficient routing. Internal compromised nodes more severe detection and correction more difficult Routing info signed by each node won't work since compromised nodes can generate valid signatures using their private keys. Detection of compromised nodes through routing information is also difficult due to dynamic topology of Ad hoc Networks. Can make use of some properties of ad hoc networks to facilitate secure routing. Routing protocols for ad hoc networks must handle outdated routing information to accommodate dynamic changing topology. False routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there are sufficient no. of valid nodes, the routing protocol should be able to bypass the compromised nodes, this however needs the existence of multiple, possibly disjoint routes between nodes. Routing protocol [5] should be able to make use of an alternate route if the existing one appears to have faulted.

II.SECURE ROUTING IN AD HOC NETWORKS

A. Problems associated with Adhoc routing:

a. Infrastructure:

An Ad hoc Network is an infrastructure less network. Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end to end routing. The nodes themselves are responsible for routing packets [6]. Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them.

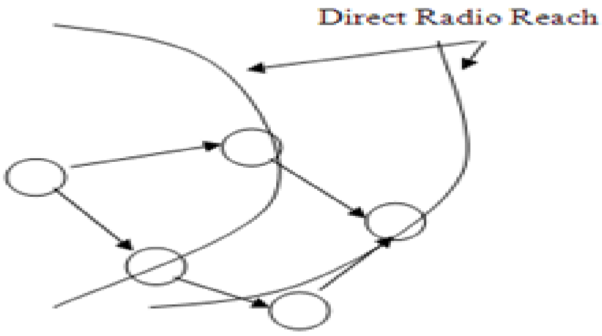

Figure 3.1 Routing in Ad hoc Network.

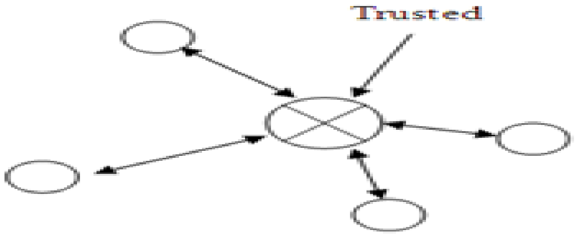

Figure 3.2 Routing in traditional network using router.

b. Frequent changes in network topology:

Ad hoc Networks contain nodes that may frequently change their locations. Hence the topology in these networks is highly dynamic [7]. This results in frequently changing neighbors on whom a node relies for routing. As a result traditional routing protocols can no longer be used in such an environment. This mandates new routing protocols that can handle the dynamic topology by facilitating fresh route discoveries.

c. Problems associated with wireless communication:

As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems [8].

d. Problems with existing Ad hoc routing protocols:

a) ***Implicit trust relationship between neighbors:*** Current Ad hoc routing protocols inherently trust all participants. Most Ad hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets. This naive trust model allows malicious nodes to paralyze an Ad hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad hoc environment magnifies this makes detection difficult.

b) ***Throughput:*** Ad hoc Networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high.

S ◄► A◄►B◄►C◄►D◄►X
↕
M

Figure. 3.3 a

S◄►A◄►B◄►M◄► C◄►D◄► X

Figure 3.4 b

c) ***Attacks using modification of protocol fields of messages:*** Current routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad hoc Networks. Since the level of trust in a traditional Ad hoc Network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS [9] attacks by simply altering these fields. For example, in the network illustrated in Figure 3.3, a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X, which C is advertising. The attacks can be classified as remote redirection attacks and denial of service attacks. Let us look at them now.

(a). Remote redirection with modified route sequence number (AODV): Remote redirection attacks are also called black hole attacks. In the attacks, a malicious node uses routing protocol to advertise itself as the shortest path to nodes whose packets it wants to intercept. Protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes towards a specific destination. In AODV, any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value. Figure 3.3 illustrates an example ad hoc network. Suppose a malicious node, M, receives the RREQ that originated from S for destination X after it is re-broadcast by B during route discovery. M redirects traffic towards itself by unicasting to B a RREP containing a significantly higher destination sequence num for X than the authentic value last advertised by X.

(b). Redirection with modified hop count (AODV): A redirection attack is also possible in certain protocols, such as AODV, by modification of the hop count field in route discovery messages [10]. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes can attract route towards themselves by resetting the hop count field of the RREP to zero. Similarly, by setting the hop count field of the RREP to infinity, routes will tend to be created that do not include the malicious node. Once the malicious node has been able to insert itself between two communicating nodes it is able to do anything with the packets passing between them.

(c). Denial of service with modified source routes: DSR is a routing protocol, which explicitly states routes in data packets. These routes lack any integrity checks and a simple denial of service attack can be launched in DSR by altering the source routes in packet headers [11]. Modification to source routes in DSR may also include the introduction of loops in the specified path. Although DSR prevents looping during the route discovery process, there are insufficient safeguards to prevent the insertion of loops into a source route after a route has been salvaged.

e. Attacks using impersonation:

Current Ad hoc routing protocols do not authenticate source IP address. A malicious node can launch many attacks by altering its MAC or IP address. Both AODV and DSR are susceptible to this attack.

f. Attacks using fabrication:

Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

(a). Falsifying route error messages in AODV or DSR: AODV [12] and DSR implement path maintenance measures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the node upstream of the link break broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. The vulnerability is that routing attacks can be launched by sending false route error messages. Suppose node S has a route to node X via nodes A, B, and C, as in Figure 3.3. A malicious node M can launch a denial of service attack against X by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and X. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for X and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to X, M can successfully prevent communications between S and X.

(b). Route cache poisoning in DSR: This is a passive attack that can occur in DSR [13] due to promiscuous mode of updating routing table which is employed by DSR. This occurs when information stored in routing table at routers is deleted, altered or injected with false information. In addition to learning routes from headers of packets, which a node is processing along a path, routes in DSR may also be learned from promiscuously received packets. A node overhearing any packet may add the routing information contained in that packet's header to its own route cache, even if that node is not on the path from source to destination. The vulnerability is that an attacker could easily exploit this method of learning routes and poison route caches. Suppose a malicious node M wanted to poison routes to node X. If M were to broadcast spoofed packets with source routes to X via itself, neighboring nodes that overhear the packet transmission may add the route to their route cache.

(c). Routing table overflow attack: In routing table overflow attack, the attacker attempts to create route to nonexistent nodes. The goal of the attacker is to create enough routers to prevent new routes from being created or overwhelm the protocol. Implementation and flush out legitimate routes from routing tables. Proactive routing algorithms attempt to discover routing information even before they are needed, while reactive algorithms create only when they are needed. This makes proactive algorithms more vulnerable to table overflow attacks.

(d). No way to detect and isolate misbehaving nodes: Misbehaving nodes can affect network throughput adversely in worst case scenarios. The existing Ad hoc routing protocols do not include any mechanism to identify misbehaving nodes. It is necessary to clearly define misbehaving nodes in order to prevent false positives. It may be possible that a node appears to be misbehaving when it is actually encountering temporary problem such as overload or low battery. A routing protocol should be able to identify misbehaving nodes and isolate them during route discovery operation.

(e). ***Easily leak information about network topology:*** Ad hoc routing protocols like AODV and DSR carry routes discovery packets in clear text. These packets contain the routes to be followed by a packet. By analyzing these packets any intruder can find out the structure of the network. The attack might use information gained to know which other nodes are adjacent to the target or the physical location of a particular node. Such an attack can be done passively. It can reveal roles of nodes in the network and their location. Intruders can use this information to attack commanded control nodes.

(f). ***Lack of self stabilization property:*** Routing protocols should be able to recover from an attack in finite time. An intruder should not be able to permanently disable a network by injecting a smaller number of mal-informed routing packets. E.g. AODV however is prone to self-stabilization problems as sequence numbers are used to verify route validity times, and incorrect state may remain stored in the routing tables for a long time.

B. Solutions to problems in Ad hoc routing Depth First Search Based Routing:

Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. To mitigate the impact of compromised nodes, we propose a suite of hybridized routing and tolerant security mechanisms with Depth first search routing based concept [14]. Based on a new cryptographic concept called pairing, we propose the notion of keys by binding private keys of individual nodes to both their IDs and locations. We also present efficient approaches to establish a shared key between any two network nodes. In contrast to previous key establishment solutions, our approaches feature nearly perfect resilience to node compromise, low communication and computation overhead, low memory requirements, and high network scalability. In this way we can eliminate the threats of attack in the ad hoc network to much more extent as required in the networks. Hence encryption and decryption can solve the problem of security threats in ad hoc networks.

III. INTRUSION DETECTION IN AD HOC NETWORKS

A. Need for intrusion detection:

The use of wireless links renders a wireless ad hoc network vulnerable to malicious attacks, ranging from passive eavesdropping to active interference. In wired networks however the attacker needs to gain access to the physical media for example network wires etc or pass through a plethora of firewalls and gateways. In wireless networks the scenario is much different, there are no firewalls and gateways in place hence attacks can take place from all directions. Every node in the ad-hoc network must be prepared for encounter with the adversary. Each mobile node in ad hoc network is an autonomous unit in itself free to move independently. This means a node with not adequate physical protection is very much susceptible to being captured, hijacked or compromised. It is difficult to track down a single compromised node in a large network; attacks stemming from compromised nodes are far more detrimental and much harder to detect. Hence every node in a wireless ad hoc network should be able to work in a mode wherein it trusts no peer. Ad hoc Networks have a decentralized architecture, and many ad hoc network algorithms rely on cooperative participation of the member nodes. Adversaries can exploit this lack of centralized decision making architecture to launch new types of attacks aimed at breaking the cooperative algorithms. Furthermore, Ad hoc routing presents more vulnerabilities than one can imagine, since most routing protocols for ad hoc networks are cooperative by nature. The adversary who compromises a ad hoc node could succeed in bringing down the whole network by disseminating false routing information and this could culminate into all nodes feeding data to the compromised node. Intrusion prevention techniques like encryption and authentication can reduce the risks of intrusion but cannot completely eliminate them for example encryption and authentication cannot defend against compromised nodes.

B. General overview:

In general terms “Intrusion” is defined as “any set of actions that attempt to compromise integrity, confidentiality or availability of the resource “Intrusion detection assumes that “user and program activities are observable “, which means that any activity which the user or an application program initiates, gets logged somewhere into system tables or some kind of a system log and intrusion detection systems (IDS) have an easy access to these system logs [15]. This logged system/ user related data is called audit data. Thus, Intrusion detection is all about capturing audit data, on the basis of this audit data determining whether it is a significant aberration from normal system behavior, if yes then IDS infers that the system is under attack. Based on the type of audit data, IDS can be classified into 2 types viz.

a. ***Network based****:* Network based IDS sits on the network gateway and captures and examines network packets that go through the network hardware interface.

b. ***Host based****:* Host based IDS relies on the operating system audit data to monitor and analyze the events generated by the users or programs on the host.

IV. CONCLUSION

We have presented an overview of the existing security scenario in the Ad hoc Network environment. Ad hoc routing aspects of wireless Ad hoc Networks were discussed. Ad hoc Networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The security protocols are still very expensive and not fail safe. Several protocols for routing in Ad hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. Intrusion detection is a critical security area. But it is a difficult goal to achieve in the resource deficient ad hoc environment. But the flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad hoc Networks wide open for research to meet these demanding application.

V. REFERENCES

[1]. Charles E. Perkins, Addison-Wesley professional, “Net Networking (paperback)”, pp.384, Issued 19 December 2000.

[2]. Eriksson L, "Security issues in Ad hoc Networks", Master's Thesis, Helsinkis University of Technology, Control Engineering Laboratories, 2004.

[3]. Z Lidong, J H Zygnumt; "Securing Ad Hoc Networks"; Cornell University, IEEE Networks, December 1999.

[4]. S. Murphy and J. J. Garcia-Luna-Aceves “An efficient routing algorithm for mobile wireless networks”, MONET, 1(2):183–197, October 1996.

[5]. B. R. Smith, S. Murphy, and J. J. Garcia-Luna-aceves. Securing distance-vector routing protocols. In Proceedings of Symposium on Network and Distributed System Security, pages 85–92, Los Alamitos, CA, February 1997. The Internet Society, IEEE Computer Society Press.

[6]. H. Bakht, M. Merabti, and R. Askwith. Centralized frame for routing in mobile ad-hoc networks. in International Conference on Computer Communication. September, 2004. Beijing, China.

[7]. Zhou L, Haas Z J, "Securing Ad hoc Networks", IEEE - Networks, 1999.

[8]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile adhoc networks: challenges and solutions,” IEEE Wireless Commun., pp. 38–47, Feb. 2004.

[9]. G. Carl, G. Kesidis, R. R. Brookes, and S. Rai. Denial-of-service attack-detection techniques. IEEE Internet Computing, 10(1):82–89, Jan/Feb 2006.

[10]. F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Wireless Mobile Networks”, 7th International workshop proceedings Springer-Verlag Berlin Heidelberg, pp.1-11, Issued 1999.

[11]. Kachirski O, Guha R, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", Knowledge Media Net., Proc. IEEE Wksp., 2002, pp. 153-58.

[12]. C. E. Perkins, E. M. Belding-Royer, and S. R. Das, “ on-demand distance vector (aodv) routing,” Internet Engineering Task Force, RFC Experimental 3561, Issued July 2003.

[13]. D. B. Johnson and D. A. Maltz. “Dynamic Source Routing in Ad-hoc Wireless Networks”,in T. Imielinksi and H. Korth editors, Mobile Computing, pp.153–181, Kluwer Academic Publishers, Issued 1996.

[14]. I. Stojmenovic, M. Russell, and B. Vukojevic, Depth first search and location based localized routing and QoS routing in wireless networks, IEEE Int. Conf. On Parallel Processing, Aug. 21-24, Toronto, 173-180.

[15]. Mishra A, Nadkarni K, Patcha A, "Intrusion Detection in Wireless Ad-Hoc Networks", IEEE Wireless Communication, February 2004, pp.48-59.

Short Bio Data for the Authors

Gavendra Kumar Sahu received the B.E. degree in Computer Science Engineering from Raipur Institute of Technology and Engineering, Raipur, in 2006, and M.Tech. in Software Engineering from Rungta College of Engineering and Technology, Bhilai, in 2011. His current research interest is to model tolerant security mechanism using DFS and GRA algorithm to reduce the energy consumption in WANET.

Neelabh Sao received B.E from Rungta College of Engineering and Technology, Bhilai, India, in the year 2003 and later did his M.Tech in CSE from Rungta College of Engineering and Technology, Bhilai, India. Currently he is working as an Assistant Professor in Rungta College of Engineering & Technology (Department of Computer Science and Engineering), Bhilai, India. His area of interest includes Data Mining.