International Journal of Computer Architecture and Mobility
(ISSN 2319-9229) Volume 1-Issue 4,February 2013

A review of Issues associated Ad-hoc routing protocols in ad-hoc Network

Puja Gupta,Jitendra Sheetlani
guptapooja2000@gmail.com,jsheetlani@gmail.com

ABSTRACT: Mobile computing is a revolutionary technology, born as a result of remarkable advances in computer hardware and wireless communication. Mobile applications have become increasingly popular in recent years. Ad-hoc networks are an emerging area of mobile computing. There are various challenges that are faced in the Ad-hoc environment.
Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. 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.
Attacks on ad hoc network routing protocols disrupt network performance and reliability with their solution. This survey paper will cover issues related to ad-hoc Network. In The paper discusses problems relevant within ad hoc networks are identified. In this article we also present ad hoc routing protocols for ad-hoc networks. The paper also gives a brief introduction to ad-hoc network, routing of ad hoc networking. .

KEYWORDS
Ad hoc networks, Security Service, Routing Protocols, Routing Authentication, Hash function and Secure Routing Protocols, MANET.

INTRODUCTION

Today advances in wireless communication technology have made mobile information services a Reality. Mobile computing is today's computing and communication area. It is a revolutionary technology, born as a result of remarkable advances in computer hardware and wireless communication. Ad Hoc Networks are complex distributed systems that consist of wireless mobile or static nodes that can freely and dynamically self-organize. In this way they form arbitrary, and temporary "Ad hoc" networks topologies, allowing devices to seamlessly interconnect in areas with no pre-existing infrastructure.
In addition to the routing challenges ad hoc networks have to face many security threats. Therefore, even routing protocols have to provide specific security mechanisms to ensure reliable and trustworthy operation. In this paper we analyzed ad-hoc routing issues.

AD-HOC NETWORK

Ad hoc networks, which are also called mesh networks, are defined by the manner in which the network nodes are organized to provide pathways for data to be routed from the user to and from the desired destination. Actually, the two names ascribed to these networks provide considerable insight. Ad hoc has two definitions—the first can be either "impromptu" or "using what is on hand," while the other is "for one specific purpose." For example, members of an ad hoc committee (studying a specific issue) might discover that they are attending the same event and decide to have an ad hoc (impromptu) meeting.

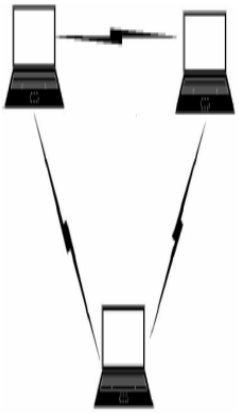

Fig. : Ad-hoc Network

Ad hoc networks follow both definitions, as well. They are formed as they are needed (impromptu), using resources on hand, and are configured to handle exactly what is needed by each user—a series of "one specific purpose" tasks.
The term mesh network accurately describes the structure of the network: All available nodes are aware of all other nodes within range. The entire collection of nodes is interconnected in many different ways, just as a physical mesh is made of many

ROUTING IN AD-HOC NETWORKS

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. 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.

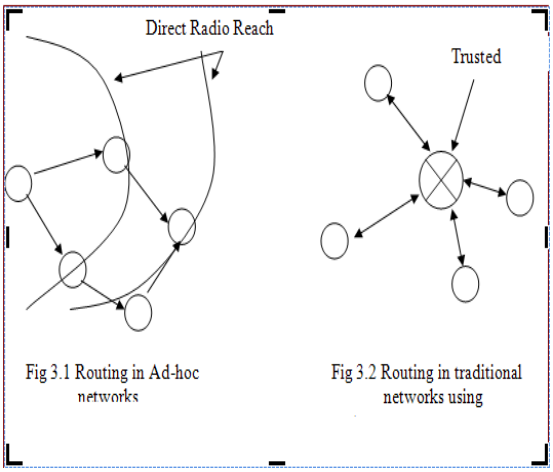

Fig 3.1 Routing in Ad-hoc networks

Fig 3.2 Routing in traditional networks using

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 dynamic and not static and should be scalable.

PROBLEMS WITH AD-HOC ROUTING PROTOCOLS

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.

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.

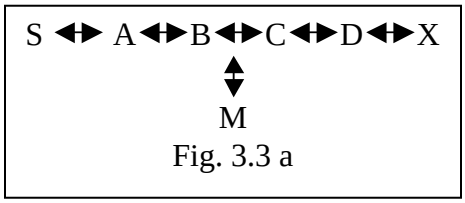

Fig. 3.3 a

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 attacks by simply altering these fields.For example, in the network illustrated in Figure3.3, 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.

SOLUTIONS TO PROBLEMS IN AD-HOC-ROUTING

Using pre-deployed security infrastructure

Here we assume existence of certain amount of security infrastructure. The type of Ad-hoc environment that we are dealing with here is called managed-open environment.

Using independent Security Agents (SA)

This method is called the Non-disclosure method (NDM). In NDM a number of independent security agents (SA) are distributed over the network. Each of

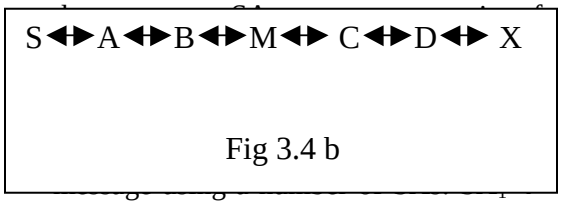

Fig 3.4 b

$SA_2 \rightarrow \ldots \rightarrow SA_N \rightarrow R$. The message is encapsulated N times using the public keys $K_{SA1} \ldots K_{SAn}$ as follows.

$$M' = K_{SA1}(SA_2, (K_{SA2} (SA_3 (\ldots(K_{SAN}(R, M))\ldots))))$$

To deliver the packet, S sends it to the first security agent SA_1 which decrypts the outer most encapsulation and forwards the packet to the next agent. Each SA knows only the address of the previous and the next hop. The last agent finally decrypts the message and forwards it to R. It introduces a large amount of overhead and hence is not preferred for routing.

Installing extra facilities in the network to mitigate routing misbehavior

Misbehaving nodes can reduce network throughput and result in poor robustness. Sergio Marti Et al propose a technique to identify and isolate such nodes by installing a watchdog and a pathrater in the Ad-hoc network on each node.

Security-Aware Ad-hoc Routing (SAR)

It makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Current routing protocols discover the shortest path between two nodes. But SAR can discover a

path with desired security attributes (E.g. a path through nodes with a particular shared key).

CONCLUSION

As the available wireless networking and mobile computing hardware is now capable of fulfilling the promise of this technology .It is the need of the hour to design and develop routing protocols which should support the performance with endurance. The correct execution of these routing protocols is mandatory for smooth functioning of a MANET. A variety of protocols have been proposed targeted at securing MANETs but no performance comparison between these protocols has previously been available. In the presented work we have compared these protocols by highlighting their features, differences and characteristics. It can be summed up that each protocol has definite advantages and disadvantages, and can be appropriate for a particular application environment.

REFERENCES

1. The global mobile information systems simulation library (glomosim). http://pcs.cs.ucla.edu/projects/glomosim .
2. W. Arbaugh, N. Shankar, and Y.C. Wan. Your 802.11 wireless network has no clothes. Technical report, Dept. of Computer Science, University of Maryland, March 2001.
3. E.M. Belding-Royer and C.-K. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communications Magazine, pages 46–55, April 1999.
4. N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
5. J. Broch, D. A. Maltz, D. B. Johnson, Y-C. Hu, , and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proc. ACM MOBICOM, pages 85–97, Oct. 1998.
6. Murat Cihan, Cetin Kaya Koc, “Setting Initial Secret Keys in Mobile Adhoc networks”, Oregoen State University, Oregon 97331, USA.