International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-1)

Research Article | **January 2015**

A Comparative Analysis on the Various Securities in Ad Hoc Networks

Er. Kailash Aseri
Research Scholar
Faculty of Engineering & Technology
Jodhpur National University,
Jodhpur, India

Mr. Om Prakash Gera
Research Scholar
Faculty of Engineering & Technology
Himalayan University,
Arunachal Pradesh, India

Abstract—

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.

In ad hoc networks the communicating nodes do not necessarily rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply. In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in more traditional networks may not directly be suitable for protecting them. A short literature study over papers on ad hoc networking shows that many of the new generation ad hoc networking proposals are not yet able to address the security problems and they face. Environment-specific implications on the required approaches in implementing security in such dynamically changing networks have not yet fully realized.

Keywords— IETF, DSDV, AODV, confidentiality, devastating, table driven.

I. INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F.

Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

Wireless networks provide rapid, untethered access to information and computing, eliminating the barriers of distance, time, and location for many applications ranging from collaborative, distributed mobile computing to disaster recovery (such as fire, flood, earthquake), law enforcement (crowd control, search and rescue) and military communications (command, control, surveillance, and reconnaissance). An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration.

In ad hoc wireless networks, every device has the role of router and actively participates in data forwarding. Communication between two nodes can be performed directly if the destination is within the sender's transmission range, or through intermediate nodes acting as routers (multi-hop transmission) if the destination is outside sender's transmission range.

As ad hoc networking somewhat varies from the more traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach somewhat restricts the set of feasible security mechanisms to be used, as the level of security and on the other hand performances are always somewhat related to each other. The performance of nodes in ad hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained, as discussed e.g. in. In addition, the available bandwidth and radio

frequencies may be heavily restricted and may vary rapidly. Finally, as the amount of available memory and CPU power is typically small, the implementation of strong protection for ad hoc networks is non-trivial.
The main objective of this paper is to give an overview of how the area of application affects the security requirements of ad hoc networks. The focus of the discussion is in the security of routing. From the requirements criteria for evaluating existing ad hoc networking solutions are formed. The evaluated proposals include the contemporary MANET drafts of the IETF. Mobile IP is not discussed.

II. SECURITY AMBITIONS

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

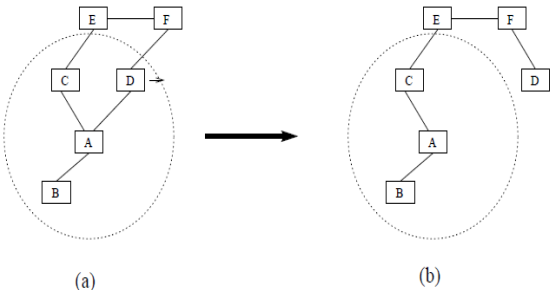

Figure 1: Topology change in ad hoc networks: nodes A, B, C, D, E, and F constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a). When node D moves out of the radio range of A, the network topology changes to the one in (b).
Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.
Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.
Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network. Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.
Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. Nonrepudiation 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 is compromised.

III. ROUTING PROTOCOLS OF AD HOC NETWORKS

Many different routing protocols have been developed for MANETs. They can be classified into two categories:
Table-driven: Table driven routing protocols essentially uses proactive schemes. They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.
On demand: A different approach from table driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined.
Three main routing protocols for a MANET are destination-sequenced distance-vector routing protocol (DSDV), AODV, and Dynamic Source Routing protocol (DSR). DSDV is a table-driven routing protocol based on the classical Bellman-Ford routing mechanism. In this routing protocol, each mobile node in the system maintains a routing table in which all the possible destinations and the number of hops to them in the network are recorded. AODV builds on the DSDV algorithm described above and is an improvement since it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in DSDV. It is an on demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. DSR is different from AODV in the sense that each mobile node keeps track of the routes of which it is aware in a route cache. Upon receiving a search request for path, it consults with its route cache to see if it contains the required information. This protocol uses more memory while reducing the route discovery delay in the system.

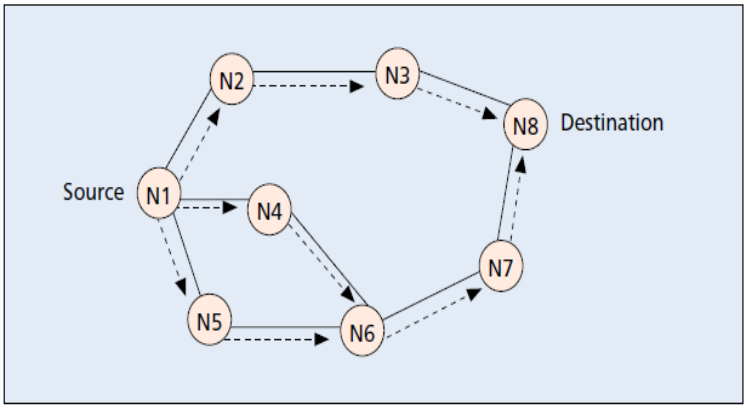

Figure 2. Propagation of RREQ.

Effective operation of a MANET is dependent on maintaining appropriate routing information in a distributed fashion. But no security is considered in currently proposed routing protocols, which makes the routing protocol an easy target for attackers.

IV. SECURITY SERVICES AND ISSUES

In order to assure a reliable data transfer over the communication networks and to protect the system resources, a number of security services are required. Based on their objectives, the security services are classified in five categories: availability, confidentiality, authentication, integrity and nonrepudiation.

1. Availability: 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.
2. Confidentiality: Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Confidentiality can be achieved by using different encryption techniques so that only the legitimate communicating nodes can analyze and understand the transmission. The content disclosure attack and location disclosure attack reveals the contents of the message being transmitted and physical information about a particular node respectively.
3. Authenticity: 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.
4. Integrity: Integrity guarantees that information passed on between nodes has not been tempered in the transmission. Data can be altered both intentionally and accidentally (for example through hardware glitches, or in case of ad hoc wireless connections through interference).

Designing a secure ad hoc wireless networks communication is a challenging task due to (1) insecure wireless communication links, (2) absence of a fixed infrastructure, (3) resource constraints (e.g. battery power, bandwidth, memory, CPU processing capacity), and (4) node mobility that triggers a dynamic network topology.

V. STANDARDS FOR PROTECTING AD HOC NETWORKS

A. Physical Security - In ad hoc networks especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However, the significance of the physical security in the overall protection of the network is highly dependent on the ad hoc networking approach and the environment in which the nodes operate. For instance in ad hoc networks that consist of independent nodes and work in a hostile battlefield the physical security of single nodes may be severely threatened. Therefore in such scenarios the protection of nodes cannot rely on physical security. In contrary, in the classroom example scenario the physical security of a node is an important issue to the owner of the node, perhaps for privacy reasons, but the breaking of the physical security does not affect the security of the system as such.

B. Security of Network Operations - The security of ad hoc networks can be based on protection in the link or network layer. In some ad-hoc solutions, the link layer offers strong security services for protecting confidentiality and authenticity, in which case all of the security requirements need not be addressed in the network or upper layers. For instance in some wireless LANs link layer encryption is applied. However in most cases the security services are implemented in higher layers, for instance in network layer, since many ad hoc networks apply IP-based routing and recommend or suggest the use of IPSec.

C. Service Aspects - Ad hoc networks may apply either hierarchical or flat infrastructure both in logical and physical layers independently. As in some flat ad hoc networks the connectivity is maintained directly by the nodes themselves, the network cannot rely on any kind of centralized services. In such networks the necessary services such as the routing of packets and key management have to be distributed so that all nodes have responsibility in providing the service. As there are no dedicated server nodes, any node may be able to provide the necessary service to another. Moreover, if a

tolerable amount of nodes in the ad hoc network crash or leave the network, this does not break the availability of the services. Finally, the protection of services against denial of service is in theory impossible. In ad hoc networks redundancies in the communication channels can increase the possibility that each node can receive proper routing information. Such approaches do, however, produce more overhead both in computation resources and network traffic. The redundancies in the communication paths, however, may reduce the denial of service threat and allow the system to detect malicious nodes from performing malicious actions more easily than in service provisioning approaches that rely on single paths between the source and destination.

D. Security of Key Management - As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As ad hoc networks significantly vary from each other in many respects, an environment-specific and efficient key management system is needed.
To be able to protect nodes e.g. against eavesdropping by using encryption, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. For very rapidly changing ad hoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumptions about a priori negotiated secrets. In less dynamic environments like in the classroom example above, the keys may be mutually agreed proactively or even configured manually (if encryption is even needed).

E. Access Control - The access control is an applicable concept also within ad hoc networking, as there usually exist a need for controlling the access to the network and to the services it provides. Moreover, as the networking approach may allow or require the forming of groups in for instance network layer, several access control mechanisms working in parallel may be needed. In the network layer the routing protocol must guarantee that no authorized nodes are allowed to join the network or a packet forwarding group such as the clusters in the hierarchical routing approach. For example in the battlefield example of the introduction the routing protocol the ad hoc network applies must control so that no hostile node can join and leave the group undetectable from the viewpoint of the other nodes in the group. In application level the access control mechanism must guarantee that unauthorized parties cannot have accesses to services, for instance the vital key management service.

VI. CONCLUSION

This paper focuses on how to secure routing and how to establish a secure key management service in an ad hoc networking environment. These two issues are essential to achieving our security goals. Besides the standard security mechanisms, we take advantage of the redundancies in ad hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. To build a highly available and highly secure key management service, we propose to use threshold cryptography to distribute trust among a set of servers. Furthermore, our key management service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way. Finally, by relaxing the consistency requirement on the servers, our service does not rely on synchrony assumptions. Such assumptions could lead to vulnerability. A prototype of the key management service has been implemented, which shows its feasibility.
In this article we study the routing security issues of MANET, analyze one type of attack, the black hole, that can easily be deployed against a MANET, and propose a feasible solution for it in the AODV protocol.
Achieving a secure routing protocol is an important task that is being challenged by the unique characteristics of an ad hoc wireless network. Traditional routing protocols fail to provide security, and rely on an implicit trust between communicating nodes.

REFERENCES

[1] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.
[2] D. P. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*, Brooks/Cole Publishing, Aug. 2002.
[3] Hubaux et al. Towards Mobile Ad Hoc WANs: Terminodes. Swiss Federal Institute of Technology, Lausanne, 2000.
[4] Jacquet, P. et al. Optimized Link-State Routing Protocol (OLSR). IETF draft, 18 July 2000.
[5] L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks," *J. Parallel Distrib. Comp.*, 2002.
[6] P. Albers *et al.*, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," *1st Int'l. Wksp. WL Info. Sys.*, *4th Int'l. Conf. Enterprise Info. Sys.*, 2002
[7] R. Kravets, S. Yi, and P. Naldurg, A Security-Aware Routing Protocol for Wireless Ad Hoc Networks, In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.
[8] S. Buchegger and J. L. Boudec, Performance Analysis of the CONFI-DANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks, In Proc. of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Jun. 2002.
[9] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, 2003.
[10] Y. -C. Hu, D. B. Johnson, and A. Perrig, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, WiSe 2003, 2003.

