To Increase efficiency in Secure Transmission using Intrusion Detection System Mitigating Routing Protocols in Mobile Adhoc NETworks (MANETS)

C.HARI KRISHNA[1] G.BALARAJU[2]

1. Assistant Professor, Anantha Lakshmi Institute of Tech & Sciences, Anantapur.
2. Assistant Professor, Anantha Lakshmi Institute of Tech & Sciences, Anantapur.

ABSTRACT

The increase in availability and popularity of mobile wireless devices has lead researchers to develop a wide variety of Mobile Ad-hoc NETworking (MANET) protocols to exploit the unique communication opportunities presented by these devices. Devices are able to communicate directly using the wireless spectrum in a peer to peer fashion, and route messages through intermediate nodes, however the nature of wireless shared communication and mobile devices result in many routing and security challenges which must be addressed before deploying a MANET. In this paper we investigate the range of MANET routing protocols available and discuss the functionalities of several ranging from early protocols such as DSDV to more advanced such as MAODV, our protocol study focuses upon works by Perkins in developing and improving MANET routing. A range of literature relating to the field of MANET routing was identified and reviewed, we also reviewed literature on the topic of securing AODV based MANETs as this may be the most popular MANET protocol. The literature review identified a number of trends within research papers such as exclusive use of the random waypoint mobility model, excluding key metrics from simulation results and not comparing protocol performance against available alternatives.

Ad Hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration, in which individual nodes cooperate by forwarding packets to each other to allow nodes to communicate beyond direct wireless transmission range. Routing is a process of exchanging information from one station to other stations of the network. Routing protocols of mobile ad-hoc network tend to need different approaches from existing Internet protocols because of dynamic topology, mobile host, distributed environment, less bandwidth, less battery power.

Keywords: MANETS, Routing Protocols, Security, Anonymity, Attacks, IDS, Watchdog

1. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this" (i.e., for this purpose). [1]

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology [1].

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz). The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

In today’s fast and rapidly growing world of technologies, more and more businesses understand the advantages of usage of computer networking. Depending on the firm’s size and resources it might be a small LAN containing only a few dozen computers; however in large corporations the networks can grow to enormous and complex mixture of computers and servers.

A computer network is a system for communication between computers. These networks may be fixed (cabled, permanent) or temporary (as via modems or null modems). Carrying instructions between calculation machines and early computers was done by human users. In September, 1940 George Stibitz used a teletype machine to send instructions for a problem set from his Model K at Dartmouth College in New Hampshire to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypes to computers was an interest at the Advanced Research Projects Agency ARPA when, in 1962, J.C.R. Licklider was hired and developed a working group he called the 'Intergalactic Network', a precursor to the ARPANet. In 1964 researchers at Dartmouth developed a time sharing system for distributed users of large computer systems. The same year, at MIT, a research group supported by General Electric and Bell Labs used a computer (DEC's PDP-8) to route and manage telephone connections. In 1968 Paul Baran proposed a network system consisting of datagrams or packets that could be used in a packet switching network between computer systems. In 1969 the University of California at Los Angeles, SRI (in Stanford), University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANet network using 50 kbit/s circuits. Networks and the technologies needed to connect and

Communicate through and between them, continue to drive computer hardware, software, and Peripherals industries. This expansion is mirrored by growth in the numbers and types of users of Networks from researchers and businesses to families and individuals in everyday use.

Since their emergence in the 1970s, wireless networks have become increasingly popular in the computing industry. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. There are currently two variations of mobile wireless networks. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. As the mobile travels out of range of one base station and into the range of another, a “handoff" occurs from the old base station to the new, and the mobile is able to continue communication seamlessly throughout the network. Typical applications of this type of network include once wireless local area networks (WLANs).

The second type of mobile wireless network is the infrastructure less mobile network, commonly known as an ad-hoc network. Infrastructure less networks has no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Example applications of ad-hoc networks are emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrains.

2. Ad-hoc Networks Versus Mobile Ad-hoc Networks

Ad-hoc networks form spontaneously without a need of an infrastructure or centralized controller. This type of peer-to-peer system infers that each node, or user, in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. These types of networks are also popularly known to as "mesh networks" because the topology of network communications resembles a mesh.

The redundant communication paths provided by ad hoc mesh networks drastically improve fault tolerance for the network. Additionally, the ability for data packets to "hop" from one user to another effectively extends the network coverage area and provides a solution to overcome non-line of sight (LOS) issues.

Mobile applications present additional challenges for mesh networks as changes to the network topology are swift and widespread. Such scenarios require the use of Mobile Ad hoc Networking (MANET) technology to ensure communication routes are updated quickly and accurately. MANETs are self-forming, self-maintained, and self-healing, allowing for extreme network flexibility. While MANETs can be completely self contained, they can also be tied to an IP-based global or local network (e.g. Internet or private networks). These are referred to as Hybrid MANETs.

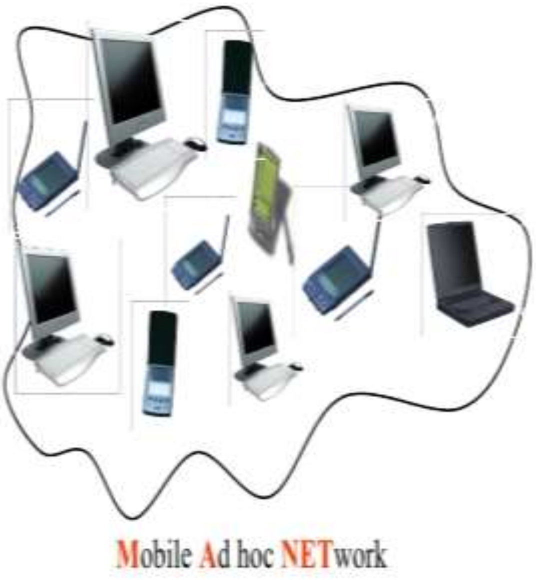
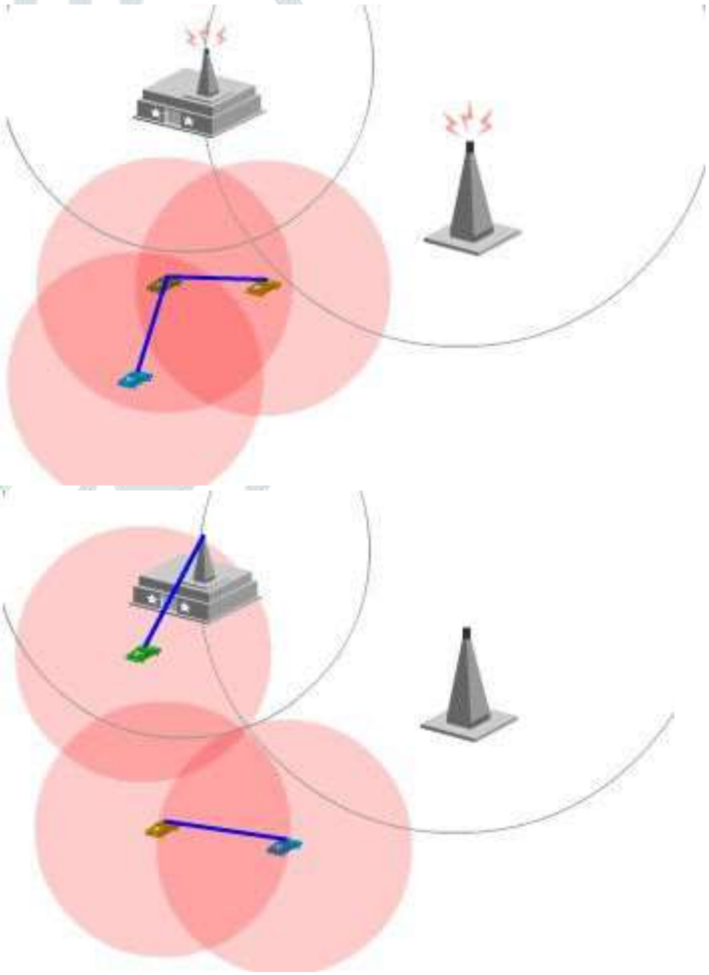


Figure 1: Mobile ad-hoc network.



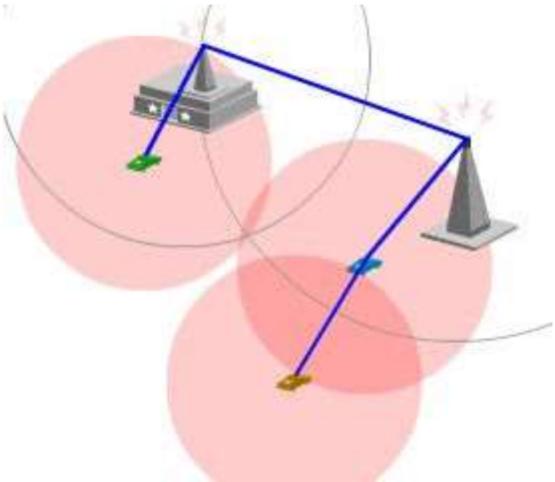


Figure 2: Hybrid Network

As you can see above we have three self-configuring mobile routers connected by wireless links creating MANET. However, as the routers approach the other two IP-based global or local networks, they form a network which connects them all through those other networks, forming a hybrid MANET.

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc.

3. HISTORY OF MANETS

The earliest MANETs were called “packet radio” networks, and were sponsored by DARPA in the early 1970s. BBN Technologies and SRI International designed, built, and experimented with these earliest systems. Experimenters included Jerry Burchfiel, Robert Kahn, and Ray Tomlinson of later TENEX, Internet and email fame. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid 1990s with the advent of inexpensive 802.11 radio cards for personal computer. Current MANETs are designed primary for military utility; examples include JTRS and NTDR.

The popular IEEE 802.11 (“Wi-Fi”) wireless protocol incorporates an ad-hoc networking
system when no wireless access points are present, although it would be considered a very low grade ad-hoc protocol by specialists in the field. The IEEE 802.11 system only handles traffic within a local "cloud" of wireless devices. Each node transmits and receives data, but does not route anything between the network's systems. However, higher-level protocols can be used to aggregate various IEEE ad-hoc networks into MANETs.

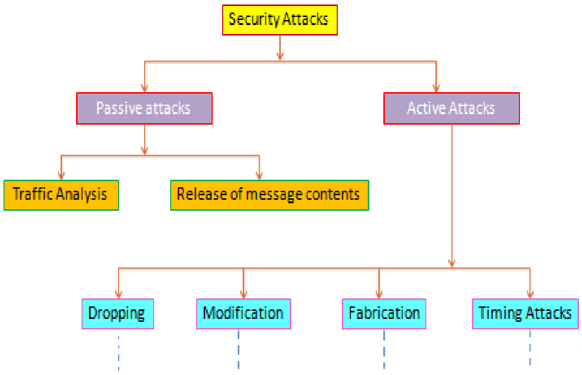
The MIT Media Lab $100 laptop program hopes to develop a cheap laptop for mass distribution (>1 million at a time) to developing countries for education. The laptops will use Adhoc wireless mesh networking to develop their own communications network out of the box.

4. BASICS OF SECURITY ATTACKS

The main two classifications of attacks in MANET are active attacks and passive attacks. These attacks are launched at the different layers of the protocol stack. Passive attacks are a continuous monitoring of the network, there is no direct damage to the network or the data. The information eavesdropped by passive attacker will used for future harmful attacks. These attackers will listen to the communication between the active nodes in the network. The active attacks cause unauthorized state changes in the MANET. In this case the attacker can stop all or parts of the data sent by the communicating parties and modify the content. The active attacks are of two kinds: internal attacks and external attacks. The internal attacks are more severe, because these attacks are caused by actively participated nodes in the network. The following diagram gives the idea about attacks on MANET

Figure 3: Security Attacks.

5. LITERATURE REVIEW



[1] Unobservable Secure routing achieves the security property of unlink ability, unobservability and anonymity by combining group signature and ID-based encryption for secure data transmission. ID based encryption depends only on the identity of the user to produce the secret key. Also using only the identity information may lead to forge the data during transmission by the trusted authority itself. At the same time the entire information about the network cannot be integrated into the single node or every node. To effectively achieve the security and to accomplish rapid transmission this paper fuses the attribute based encryption technique with Better Approach To Mobile Ad-hoc Networking, or B.A.T.M.A.N. which is a routing protocol that maintains the best hop information in its routing table. This technique only needs to know the next hop details rather than knowing about the entire network details. Each node maintains the direction from which it receives the data and to which it sends the data. Attribute based encryption preserves the identity of the nodes participating in the network. This scheme prevents adversaries to modify the contents, also protects adversaries against tracing the source and the destination identity. From this we are accomplishing rapid transmission of data in a protected way with minimum node failure rate.

In this paper, we have proposed an anonymous secure routing protocol using BATMAN and Attribute based encryption. The proposed scheme provides fast and secure transmission. In this method the intelligence of BATMAN which maintains only the best next hop so it reduces the computation without maintaining the entire network details. The encryption part secures the data from the attackers. This method uses access policies to validate the data during transmission of the data. There are adversaries present in the network who have monitoring the data transmitted in the network. This method preserves the confidentiality of the data even though the node is compromised by the adversary.

[2] As the nodes in MANET are battery limited, one node per cluster is elected as leader to run IDS for all the nodes in the cluster. Leader is elected based on the residual energy of each node that is sufficient to run IDS. Too much of resources are wasted for the implementation of intrusion detection scheme for every node. Hence nodes are grouped into cluster and cluster head is elect to serve other node in network, where as selfish node with maximum resources are not nominated for cluster head selection, because of self interest to save its own power. Nodes are provided incentives in the leader election process by VCG mechanism for preventing the nodes from exhibiting the selfish behaviour.1) To ensure security and to detect the intrusion in Mobile Ad hoc networks select a leader from the 1hop cluster as cluster head contains most resource.2)To avoid the issues arise due to optimal collection of leader and performance overhead, a solution is Mechanism based design theory.3)The solution provides nodes with incentives in the form of reputations to encourage nodes in honestly participating in the election process.

The proposed work specifies that intrusion detection based on clustering and leader election technique considerably reduces the resource consumption and detects the intrusion. An unbalanced resource consumption of IDSs in MANET and the presence of selfish nodes have motivated to an integrated solution for prolonging the lifetime of mobile nodes and for preventing the emergence of selfish nodes. The solution motivated nodes to truthfully elect the most cost efficient nodes that handle the detection duty on behalf of others. Moreover, the sum of the elected leaders is globally optimal. To achieve this goal, incentives are given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis. Reputations are computed using the well known VCG mechanism by which truth-telling is the dominant strategy. We analyzed the performance of the mechanisms in the presence of selfish and malicious nodes. To decrease the percentage of leaders, single node clusters, maximum cluster size and increase average cluster size. These properties allow improving the detection service through distributing the sampling budget over less number of nodes and reduce single nodes to launch their IDS.

[3] Put in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies\ misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

[4] An ad hoc network is a collection of wireless computers (nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed trusted environment. In this paper, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

[5] In this paper, we have presented the design and evaluation of SEAD, a new secure ad hoc network routing protocol using distance vector routing. Many previous routing protocols for ad hoc networks have been based on distance vector approaches but they have generally assumed a trusted environment. Instead, in designing SEAD, we carefully fit inexpensive cryptographic primitives to each part of the protocol functionality to create an efficient, practical protocol that is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. Together with existing approaches for securing the physical layer and MAC layer within the network protocol stack, the SEAD protocol provides a foundation for the secure operation of an ad hoc network.

We base the design of SEAD in part on the DSDV ad hoc network routing protocol and in particular, on the DSDV-SQ version of the protocol, which has been shown to outperform other DSDV versions in previous detailed ad hoc network simulations. For security, we use efficient one-way hash functions and do not use asymmetric cryptographic primitives. Consequently, SEAD is efficient and can be used in networks of computation- and bandwidth-constrained nodes.

SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio, although it does create more overhead in the network, both due to an increased number of routing advertisements it sends, and due to the increase in size of each advertisement due to the addition of the hash value on each entry for authentication.

In future work, we plan to also consider mechanisms to detect and expose nodes that advertise routes but do not forward packets, and to merge this work with our other work in securing on-demand routing protocols to create a secure protocol based on ZRP. We are also considering the possibility of extending DSDV to behave like a path-vector routing protocol, allowing the source address of each advertisement to be more readily authenticated.

CONCLUSION AND FUTURE WORK

In this paper, we have proposed an anonymous secure routing protocol using BATMAN and Attribute based encryption. The proposed scheme provides fast and secure transmission. In this method the intelligence of BATMAN which maintains only the best next hop so it reduces the computation without maintaining the entire network details.

An unbalanced resource consumption of IDSs in MANET and the presence of selfish nodes have motivated to an integrated solution for prolonging the lifetime of mobile nodes and for preventing the emergence of selfish nodes. The solution motivated nodes to truthfully elect the most cost efficient nodes that handle the detection duty on behalf of others.

We show that the two techniques increase throughput by 17% in a network with moderate mobility, while increasing the ratio of overhead transmissions to data transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the percentage of overhead transmissions from 12% to 24%

Instead, in designing SEAD, we carefully fit inexpensive cryptographic primitives to each part of the protocol functionality to create an efficient, practical protocol that is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. Together with existing approaches for securing the physical layer and MAC layer within the network protocol stack, the SEAD protocol provides a foundation for the secure operation of an ad hoc network. We base the design of SEAD in part on the DSDV ad hoc network routing protocol, and in particular, on the DSDV-SQ version of the protocol, which has been shown to outperform other DSDV versions in previous detailed ad hoc network simulations

REFERENCES

[1] Balaji. S, Manicka Prabha. M,"AUST: Anonymous Unswerving and Secure Transmission in MANET," International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 3, pp.60-64, March 2013.

[2] Kalaivani.R,RamyaDorai.D," Secure Protocol for Leader Election and Intrusion Detection in

MANET," International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3, Issue 3, pp.62-66, March 2013.

[3] Alberto Rodriguez-Mayol, Javier Gozalvez, " Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks," Proceedings of the European Wireless Conference, 2010.

[4] S. Marti, T. J. Giuli, K. Lai, M. Baker, “Mitigating routing misbehavior in mobile ad-hoc networks,” Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing And Networking, pp 255-265, Aug. 2000.

[5] Yih-Chun Hu, David B. Johnson, Adrian Perrig, ” SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks,”Journal: Ad Hoc Networks , vol. 1, no. 1, pp. 175-192, 2003.

Authors:

C.HARI KRISHNA **M.Tech [AI]**
As an Assistant Professor in the department of computer science and engineering, **ALTS**, Anantapuramu. He received from **B.Tech** Degree in the Department of Computer Science and Engineering, **JNTU-Anantapuramu** from **2007-2011**. He received from **M.Tech** degree in Artificial Intelligence Specialization from **JNTU Anatapuramu** from **2012-2014**.

G.BALARAJUM.TECH [CS]**

As an Assistant Professor in the department of computer science and engineering, **ALTS**, Anantapuramu. He received from **B.E** Degree in the Department of Information Science and Engineering **VTU**, **Belgavi, 2007-2011**. He received from **M.Tech** degree in Computer Science and Engineering from **REVA Engineering College, Bangalore**, **2012-2014**