Survey of Secure Routing Protocols for MANETs (MOBILE ADHOC NETWORKS)

*Ajay Sharma, *Nithesh K. Nandha, **Kailash Parik, ***Prof. K.P. Yadav

*Research Scholar, Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan, India
** Research Scholar, Singhania University, Rajasthan, India
***Professor, SIET, Ghaziabad, U.P., India

ABSTRACT

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 measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. Network sizes and occurrences increased creating a requirement for inter-network communication. Research on MANETs has nearly 20 years focused on routing and this focus still remains. Several routing protocols for MANETs have been proposed and some surveys on these protocols have been published (2010) and an IETF Routing Area Working Group MANET (Mobile, 2011) has been active for a decade with six currently active Internet drafts.

Key Words: MANET, IDS, DoS, RTT.

1.INTRODUCTION

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 measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. Network sizes and occurrences increased creating a requirement for inter-network communication. This led to the development of the Internet and its suite of protocols. The use of the Internet and its applications became ubiquitous. Research on MANETs has nearly 20 years focused on routing and this focus still remains. Several routing protocols for MANETs have been proposed and some surveys on these protocols have been published (2010) and an IETF Routing Area Working Group MANET (Mobile, 2011) has been active for a decade with six currently active Internet drafts. The following issues are main in this area:

a) **Security-** Mobile ad-hoc network is a relatively new innovation in the field of wireless technology. These types of networks operate in the absence of fixed infrastructure, which makes them easy to deploy at any place and at any time. The absense of any fixed infrastructure in mobile ad-hoc networks makes it difficult to utilize the existing techniques for network services, and poses number of various challenges in the area. Typical challenges include routing, bandwidth constraints, security and power. Routing can be defined as a mechanism of information exchange between two hosts in a network. It plays an important role to ease communication between different parties within the network. There are various proposed routing solutions for mobile ad-hoc networks. As I discussed in the previous article, some of these solutions are table-driven, on-demand, geographical, geographical multicast and multicast. Most of these solutions mainly focus on routing and do not concentrate much on other related issues, such as security.

b) **Protocol-** Routing protocols can also be classified as link state protocols or distance-vector protocols. Routers using a link state routing protocol maintain a full or partial copy of the network topology and costs for all known links. Routers using a distance-vector protocol keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Generally speaking, “link state routing protocols are more reliable, easier to debug and less bandwidth-intensive than distance-vector” protocols. Link state protocols are also more complex and more compute- and memory-intensive. There are some previous protocols, such as the Source Tree Adaptive Routing (STAR) protocol and the Partial Tree-Sharing

Protocol (PTSP), which are not the focus of active investigation now and their ideas are similar to more recently proposed protocols, such as the Topology Broadcast Based on Reverse-Path Forwarding (TBRPF) protocol.

c) **Benefits -**There are several advantages of manets as it is wireless connection for information transfer from one place to another place with a very high speed and in huge amount of capacity which was unpredictable few years back. Transfers of real pictures have become activities of live telecast any incident to remote places.

d) **Categories-**There are different types of MANETs including:

InVANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.

Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.

2.SCOPE OF THE PROPOSED STUDY

Future mobile ad-hoc networks will use mobile routers to provide Internet connectivity to mobile ad-hoc users. A mobile router will also allow mobility of an ad-hoc network, where mobile users may use an Internet access within an ad-hoc network domain. Recently, organizations have begun to see potential for such dynamic networks. Mobile ad-hoc networks are of increasing interest for a distributed set of applications, such as distributed collaborative computing, distributed sensing networks, potential fourth/fifth generation wireless systems, and response to incidents that destroyed the existing communication structure.

There is current and future need for dynamic ad-hoc networking technology. The emerging field of mobile computing, with its current focus on mobile IP operation, will expend gradually. In the future, mobile computing will require highly-adaptive networking technology to manage multi-hop clusters that can operate autonomously and possibly be able to attach at some point to the bigger network.

Wireless networks can be deployed in either infrastructure-based mode or on an ad-hoc basis. Although work is being done and prototype protocols are available for experiments, mobile ad-hoc networks still have difficulties. While some basic network control functions and routing procedures have been developed, many other issues require attention. Rapidly changing topology, network partitions, higher error rates, collision interference, bandwidth constraints, and power limitations together pose new challenges in network control; especially in the design of higher level protocols for routing and in implementing applications with quality of service requirements.

3.RESEARCH GAPS IDENTIFIED IN THE PROPOSED FIELD OF INVESTIGATION

An Intrusion Detection System (IDS) detects malicious and selfish nodes in a network. Ad hoc networks are often secured by using either intrusion detection or by secure routing. Designing efficient IDS for wireless ad-hoc networks that would not affect the performance of the network significantly is indeed a challenging task. Arguably, the most common thing in a review paper in the domain of wireless networks is to compare the performances of different solutions using simulation results. However, variance in multiple configuration aspects including that due to different underlying routing protocols, makes the task of simulation based comparative evaluation of IDS solutions somewhat unrealistic. Instead, the authors have followed an analytic approach to identify the gaps in the existing IDS solutions for MANETs and wireless mesh networks.

Mobile multi-chip ad hoc networks are collections of mobile nodes connected together over wireless medium. These nodes can freely and dynamically self-organize into arbitrary and temporary, “adhoc” network topologies, allowing people and devices to seamlessly internet work in areas with no preexisting communication infrastructure .In spite of the massive research efforts, mobile adhoc networks have not yet affected our way of using wireless networks. Currently, mobile ad hoc networks are applied only in either battlefield scenarios (large-scale military applications with thousands of mobile ad hoc nodes) or specialized civilian applications (disaster recovery, planetary exploration, etc). While WiFi technology is now ubiquitous, users seldom operate 802.11 cards in ad hoc mode and, except laboratory test beds; they never use multi-chip ad hoc networks. This is due to

several reasons: applications (lack of), systems implementation and integration (lack of), and experimentation (lack of).

4.OBJECTIVES OF THE PROPOSED STUDY

Our primary objectives are:
1) To analyze and survey of secure routing protocols for MANETs
2) To implement and evaluate CONFIDANT protocols to demonstrate how the dynamic feedback mechanisms improve the network performance and what are the side effects of introducing the mechanism to the mobile ad hoc network.
3) To design a protocol for the distribution of reputation data based analysis.

To solve the problem, the following sub-objectives can be seen:
1) To investigate security issues of mobile ad hoc network and current dynamic feedback mechanisms or protocols that are used to solve or mitigate the issues.
2) To investigate and learn how to use the network simulation tool. There are several popular network simulation tools available and we need to choose the one that best suits our needs. The selected network simulator should be studied so that we can use it as platform to implement protocol and conduct simulations.
3) To analyze and implement the CONFIDANT protocol based on Dynamic Source Routing protocol (DSR); evaluate the network performance.

5.RESEARCH METHODOLOGY

Most current ad hoc routing protocols assume that the wireless network is benign and every node in the network strictly follows the routing behavior and is willing to forward packets for other nodes. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes present in the network. A commonly observed misbehavior is packet dropping. Practically, in a MANET, most devices have very limited computing and battery power while packet forwarding consumes a lot of such resources. Thus some of the mobile devices would not like to forward the packets for the benefit of others and they drop packets not destined to them. On the other hand, they still make use of other nodes to forward packets that they originate. These misbehaved nodes are very difficult to identify because we cannot tell that whether the packets are dropped intentionally by the misbehaved nodes or dropped due to the node having moved out of transmission range or other link error. Packet drop significantly decreases the network performance.

Hypotheses to be tested: Denial-of-Service (DoS) attacks pose a major threat to the availability of wireless ad hoc networks. Fault tolerant operation of wireless ad hoc networks will depend on the placement of DoS countermeasures in sufficiently robust form. DoS attack called the *Stasis Trap* attack, and propose a technique for detecting such an attack. Stasis Trap attack has two distinguishing characteristics—it has across-layer design, and is stealthy. The Stasis Trap attack has across-layer design in that it is launched from the MAC layer butts aim is to degrade the end-to-end throughput of flows at the transport layer by exploiting TCP's congestion-control mechanism. Specifically, an adversary launches a Stasis Trap attack against neighboring nodes by periodically preempting the wireless channel in order to cause large variations in the roundtrip time (RTT) of TCP flows. Channel preemptions are carried out by manipulating the back-off mechanism of the Distributed Coordinating Function of the 802.11 MAC protocol. The periodic preemptions induce large RTT variations in the TCP flows that are within the transmission range of the adversary. This in turn causes a significant drop in the throughput of those flows, thereby creating a "stasis trap" around the adversary that entangles TCP flows. The aforementioned attack severely degrades end-to-end throughput but has very little effect on MAC-layer throughput, and hence it is very hard to detect at the MAC layer, which is its point of attack. In this sense, this attack is stealthy.

6.TOOLS AND TECHNIQUES OF RESEARCH

(1) Hashing techniques available are based on the concept of a hash function that transforms a given input of arbitrary length to a value of a fixed length, called the hash value. The transformation is done in a manner that it is computationally infeasible to transform the hash value to the original value. Hash functions are very efficient as they do not involve heavy computations and hence are applied in the area of security for message authentication and integrity checks. The problem with hash functions is collision. Collision is a situation where a hash function generates the

same hash value for more than one different input values. Collisions are possible in a hash function due to the fact that it transforms an input of any length to an output of fixed length, meaning a mapping from a larger set to a smaller set. The solution to this problem is achieved through the adoption of appropriate collision resolution or avoiding techniques. There can be three ways in which the collisions can be handled: first by selecting a hash function that is more and more collision resistant, second by putting the processing in an environment to minimize the chance of collisions and third by resolving when the collision really takes place. The choice of a hash function, its implementation and its associated collision resolution technique depends on problem area that is being solved.

(2) One reason is the high complexity involved in implementing and testing actual ad-hoc networks, and the lack of software tools for doing so. We have thus built an inexpensive and flexible environment to support such tasks and to facilitate network research. The core component is a mobility emulator to test an ad-hoc network of virtually any scale and with any mobility scenario without actually moving the nodes physically**.**

(3) A wireless intrusion detection tested comprised of six ad hoc nodes, including four Dell Latitude C600 laptops and two Sony Vaio laptops, was set up for all the tests. The Dell laptops have Mobile Pentium III-750 MHz processors and 128MB of RAM, and the Sony laptops have Mobile Pentium IV-1.6 GHz processors and 512MB RAM. All the laptops had the Linux operating system and ran the UCSB AODV implementation [4]. For wireless connectivity, Lucent Orinoco and NETGEAR IEEE 802.11b wireless cards were used. The laptops were physically co-located and the connectivity was controlled using ip tables for MAC layer filtering. This provided a controllable environment in which AODVSTAT could be tested. One of the nodes in the ad hoc network acted as an AODVSTAT intrusion detection sensor. During all the experiments, the sensor nodes participated in the AODV routing protocol. For each experiment, data traffic consisted of 512-byte UDP packets. The transmission rate for data packets was set at ten packets per second.

7.CONCLUSION & FUTURE SCOPE

In the last few years, the performance and use of wireless technologies has increased tremendously, opening up avenues for applying these in previously less explored areas. One such field concerns mobile ad hoc networks (MANETs) in which mobile nodes organize themselves in a network without the help of any predefined infrastructure. Securing MANETs is an important part of deploying and utilizing them, since they are often used in critical applications where data and communications integrity in important. Existing solutions for wireless networks can be used to obtain a certain level of such security.

The best of our knowledge, the study is the first that will uses information scoring and ranking as classification key. According to this key, approaches can be classified as based on information theory, clusters and social network theory, and cooperative and non-cooperative game theory. It also provides a common nomenclature for all of them. The main contribution of the research is to provide an analysis of the most representative approaches and present a novel qualitative comparison.

Today, the mushrooming of heterogeneous wireless technologies and the need of robust and efficient communication systems are essence for the ubiquitous and integrated wireless infrastructure. Progress in the theoretical underpinnings of embodied intelligence may have strong techno-logical implications in areas like robotics, actuator technology, materials, self-assembling, systems data processing, business and finance, smart phones, expert systems, customer trouble-shooting services, education and e-learning, network system diagnostics, network maintenance and repair, network monitoring and protection programs. This has expanded view takes into account the fact that intelligence and control is becoming more distributed throughout the network. Wireless networks are more prone to physical threats, so there is a need to provide a secure authentication interface and to apply proven security measures to protect network traffic between the wired network and wireless devices. Due to enhancement in network technology scalability is one of the major important factor.

REFERENCES

[1]C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks, Architectures and Protocols,” first Indian reprint 2005,pearson publication. ISBN 81-297-0945-7

[2]Henrik Lundgren“Implementation and experimental evaluation of wireless ad hoc routing protocol,” Acta Universitet upsaliensis-uppsala,2005.

[3]Dr. Yogesh Chaba and Naresh Kumar Medishetti, " Routing protocols in Mobile Ad hoc Networks-A Simulation Study Final", JCS Vol1,No.1, August 2005.

[4]Paolo Santi "Topology Control in Wireless Ad hoc and Sensor Networks",John Wiley & Sons.Ltd,2005.

[5]Cordasco, J., & Wetzel, S. (2007). Cryptographic vs. trust-based methods for MANET routing security. Electronic Notes in Theoretical Computer Science, Elsevier, 197(2), 131-140. Retrieved December 11, 2011 from http://www.cse. msstate.edu/ ~ramkumar/cryptvstrust.pdf

[6]Djenouri, D., & Badache, N. (2010). Security in mobile ad hoc networks. Germany: LAP Lampert Aca-demic Publishing.

[7]Garg, N., & Mahapatra, R. P. (2009). MANET security issues. IJCSNS International Journal of Computer Science and Network Security, 9(8).

[8]Goyal, T., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications, 9(12), 11-15.

[9]Hu, Y., & Johnson, D. B. (2004). Securing quality-of-service route discovery in on-demand routing for ad hoc networks. Proceedings of ACM SASN'04.

[10]Johnson, D., Hu, Y., & Malz, D. (2007). The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. IETF, Request for Comments (RFC) 4728.

[11]Karlsson, J., Dooley, L.S., & Pulkkis, G. (2011). A new MANET wormhole detection algorithm based on traversal time and hop count analysis. Sensors, 11 (12), 11122-11140. Retrieved December 11, 2011 from http://www.mdpi.com/1424-8220/11/12/11122/pdf

[12]Khabbazian, M., Mercier, H., & Bhargava, V.K. (2006). Wormhole attack in wireless ad hoc networks: Analysis and countermeasure. Proceedings of Global Telecommunications Conference, GLOBE-COM'06, IEEE.

[13]Li, X., Lyu, M. R., & Liu, J. (2004). A trust model based routing protocol for secure ad hoc networks. Pro-ceedings of Aerospace Conference, Vol. 2, USA: IEEE Press. 1286-1295, ISBN 0-7803-8155-6.

[14]Liu, C., & Kaiser, J. (2005). A survey of mobile ad hoc network routing protocols. MINEMA (Middleware for Network Eccentric and Mobile Applications) Scientific Programme Report TR-4, University of Magdeburg, Germany. Retrieved December 7, 2011 from http://www.minema.di.fc.ul.pt/reports/report_routing-protocols-survey-final.pdf

[15]Liu, J., Fu, F., Xiao, J., & Lu, Y. (2007). Secure routing for mobile ad hoc networks. Proceedings of Eight ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Par-allel/Distributed Computing.

[16]Mobile Ad-hoc Networks (MANET). (2011). IETF Routing Area Working Group. Retrieved December 7, 2011 from http://datatracker.ietf.org/wg/manet/charter

[17]Mohseni, S.,Hassan, R., Patel, A., & Razali, R. (2010). Comparative review study of reactive and proactive routing protocols in MANETs. Proceedings of 4th IEEE International Conference on Digital Ecosys-tems and Technologies, Abu Dhabi, United Arab Emirates.

[18]Patmaik, G. K., & Gore, M. M. (2011). Trustworthy path discovery in MANET – A message oriented cross-correlation approach. Proceedings of 2011 Workshops of International Conference on Advanced Information Networking and Applications (WAINA). USA: IEEE Press, 170-177.

[19]Perrig, A., Song, D., Canetti, R, Tygar, J. D., & Briscoe, B. (2005). Timed efficient streamless-tolerant au-thentication. IETF, Request for Comments (RFC) 4082.

[20]Pirzada, A. A., & McDonald, C. (2004). Establishing trust in pure ad-hoc networks. Proceedings of 27th Australasian Computer Science Conference. Retrieved December 11, 2011 from http://crpit.com/confpapers/CRPITV26Pirzada1.pdf

[21]Pushpa, A. M. (2009). Trust based secure routing in AODV routing protocol. Proceedings of 2009 Interna-tional Conference on Internet Multimedia Services Architecture and Applications (IMSAA), USA: IEEE Press, 1-6 .

[22]Ramana, K. S., Chari, A. A., & Kasiviswanth, N. (2010). A survey on trust management for mobile ad hoc networks. International Journal of Network Security & Its Application (IJNSA), 2(2), 75-85. Retrieved December 10, 2011 from http://airccse.org/journal/nsa/0410ijnsa6.pdf

[23]Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. Proceedings of the 10th International Conference on Network Protocols (ICNP'02).

[24]Singh, U. (2011). Secure routing protocol in mobile ad hoc networks – A survey and taxonomy. Interna-tional Journal of Reviews in Computing, 7(2), 9-17. Retrieved December 10, 2011 from http://www.ijric.org/volumes/Vol7/Vol7No2.pdf

[25]Taneja S., & Kush, A. (2010). A survey of routing protocols in mobile ad hoc network. International Jour-nal of Innovation, Management and Technology, 1(3), 279-285.

[26]Tomar, P., Suri, P. K., & Soni, M. K. (2010). A

comparative study for secure routing in MANET. Interna-tional Journal of Computer Applications, 4(5), 17-22.

[27]Wang, D., Hu, M., & Zhi, H. (2008). A survey of secure routing in ad hoc networks. Proceedings of the Ninth International Conference on Web-Age Information Management WAIM '08, USA: IEEE Press, 482-486.