A Study of Security Challenges in Mobile Ad hoc Networks

G. Shanthi [1]
Research Scholar,
Bharathiar University, Coimbatore

Dr. M. Ganaga Durga [2]
Research Coordinator,
Bharathiar University, Coimbatore

***Abstract*— Mobile ad hoc networks (MANETs) are constructed of composite distributed systems which comprise wireless nodes and particularly useful in places where network infrastructure is costly. Protecting MANETs from security threats is a challenging task because of the MANETs dynamic topology. Every node in a MANETs is independent and is free to move in any direction, therefore change its connections to other nodes occurred frequently. Due to its decentralized nature, different cases of attempts can be taken place. The purpose of this research report is to analyze different MANETs security attacks.**

Keywords: MANETs, Routing protocols, Attacks, Cryptography

1. INTRODUCTION

From last some years not only mobile devices are becoming smaller, more punk, more convenient, and more configured, they also run more applications and network services which increasing the development of mobile computing equipment market. Projections indicate that in the next couple of years the number of fluid connections and the number of consignments of mobile and Internet terminals will grow yet by another 20–50% [1].

A mobile ad hoc network (MANET) is a collection of mobile devices that can pass by each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robotic networks, and so on. Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [2].

1.1 Ad hoc networking issues

Ad-hoc networks are a fresh paradigm of wireless communication for mobile hosts. In that respect is no set up infrastructure such as base stations for mobile switching. Nodes within each other's radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems. The following Fig 1 shows the operating process of ad hoc network.

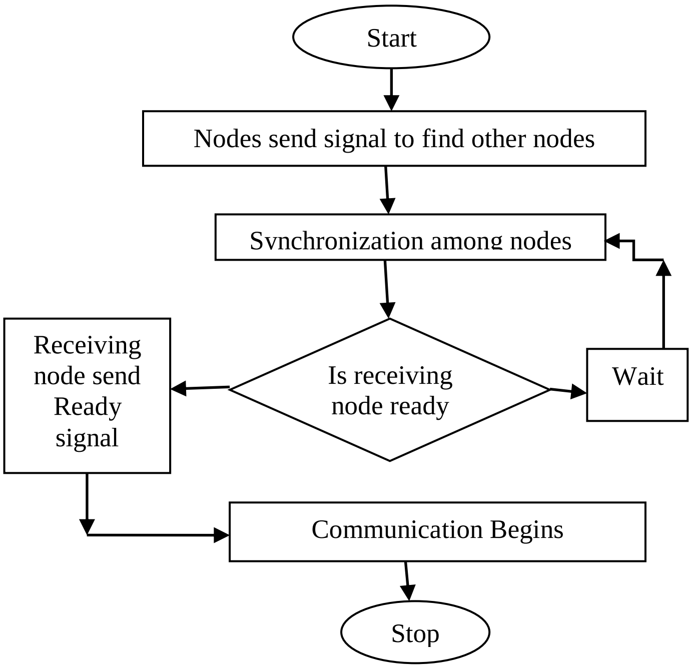
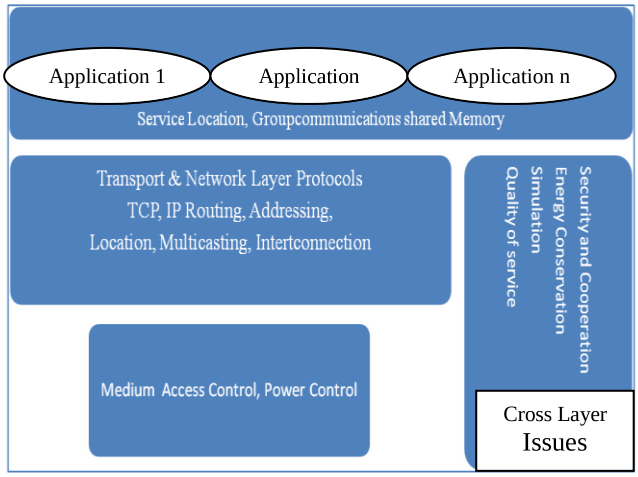

Start
Nodes send signal to find other nodes
Synchronization among nodes
Is receiving node ready
Wait
Receiving node send Ready signal
Communication Begins
Stop

Fig 1 Working Procedure Ad hoc Networks

There are some specific MANET issues and constraints which create evils and significant challenges in the ad hoc network. To show the enormous sum of research activities on ad hoc networks in a methodical manner, we will use them, as a hint. The simplified architecture shown in following Fig 2.

As depicted in the Figure, the research activities will be combined, according to a layered approach into three primary regions:

• Enabling Technologies; • Networking; • Middleware and applications.


Application 1
Application
Application n
Service Location, Groupcommunications shared Memory
Transport & Network Layer Protocols
TCP, IP Routing, Addressing,
Location, Multicasting, Intertconnection
Medium Access Control, Power Control
Security and Cooperation
Energy Conservation
Simulation
Quality of service
Cross Layer
Issues

.

Fig 2 Simplified Architecture

The development of MANET cannot be separated from the universe of computing. Since it is portable and compact media with which we can communicate exclusive of a wired net. In this review paper, we talked over some typical and dangerous vulnerability in the MANET, attack type security criteria, which move on to supply guidance to the security-related research works in this field.

1.2 *Characteristics of MANET*

Autonomous and infrastructure less: MANET is a self-organized network, independent of any established infrastructure and centralized network administration. Each node acts as a router and operates in a distributed manner.

Multi-hop routing: Since there exists no dedicated outer, then every node as well acts as a router and aids in forwarding packets to the designated goal. Hence, data sharing among mobile nodes is made available.

Dynamic network topology: Since MANET nodes move randomly on the net, the topology of MANET changes frequently, leading to regular route changes, network partitions, and possibly packet losses.

Variation on link and node capabilities: Every participating node in an ad hoc network is equipped with a dissimilar type of radio devices having varying transmission and receiving capabilities. They all operate on multiple frequency bands. Asymmetric links may be made due to this heterogeneity in the radio capabilities. **Energy-constrained operation:** The processing power of node is restricted because the batteries carried by portable mobile devices have fixed power supply.

Scalability: A wide range of MANET applications may call for bulky networks with mass of nodes, especially that can found in strategic networks. Scalability is essential to the flourishing operation of the MANET.

2. ROUTING PROTOCOLS

MANET routing protocols are categorized into three main categories depending upon the criteria when the source node possesses a route to the destination, as shown in the following tree structure Fig 3.

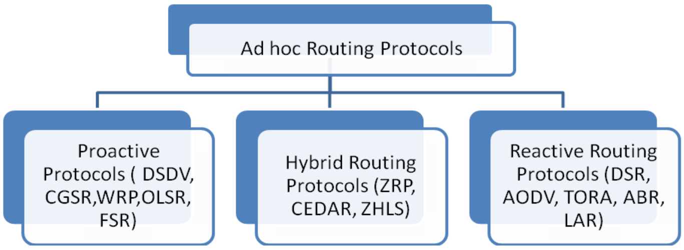

Ad hoc Routing Protocols
Proactive Protocols (DSDV, CGSR,WRP,OLSR, FSR)
Hybrid Routing Protocols (ZRP, CEDAR, ZHLS)
Reactive Routing Protocols (DSR, AODV, TORA, ABR, LAR)

Fig 3 Routing Protocols

2.1 *Proactive Routing Protocols*

The proactive protocols maintain reliable and up to date routing information between all the clients in an ad hoc network. In this each node builds its own routing table which can be utilized to find out a path to a destination and routing data is stacked away. Whenever there is any variation in the mesh topology, updating has to be established in the entire network [7]. More or less of the main table driven protocols are:

- Optimized Link State Routing protocol (OLSR)
- Destination sequenced Distance vector routing (DSDV)
- Wireless routing protocol (WRP)
- Fish eye State Routing protocol (FSR)
- Cluster Gateway switch routing protocol (CGSR)

2.2 *Reactive Routing Protocols*

In On-demand or Reactive routing protocols routes are formed as and when required. When a client wants to commit information to any other node, it first initiates route discovery process to find out the route to that destination node. This path remains applicable till the destination is accessible or the route is not wanted. Dissimilar types of on demand driven protocols have been developed such as:

- Ad hoc On Demand Distance Vector (AODV)
- Dynamic Source routing protocol (DSR)
- Temporally ordered routing algorithm (TORA)
- Associativity Based routing (ABR)

2.3 *Hybrid Routing Protocols*

This case of routing protocols combines the characteristics of both the former classes. The nodes belonging to a particular geographical region are believed to be in the same zone and are proactive in nature. Whereas the communication between nodes located in different zones is done reactively. The different types of Hybrid routing protocols are:

- Zone routing protocol (ZRP)
- Zone-based hierarchical link state (ZHLS)
- Distributed dynamic routing (DDR)

2.4 *AODV*

It is a reactive routing protocol designed for a mobile ad hoc network. In AODV [8], when a source node S wants to transport a data package to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbours who receive this RREQ rebroadcast the same RREQ to their neighbours. This procedure is iterated until the RREQ reaches the goal client. Upon meeting the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be brushed aside by the destination client. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or larger than the one in the RREQ) to generate and send a RREP to the root node.

2.4 OLSR

It is a proactive routing protocol, that it is founded on the periodic exchange of topology information. The central concept of OLSR is the use of multipoint relays (MPR) to supply an efficient flooding mechanism by reducing the number of transmissions required. In OLSR [9] each node selects its own MPR from its neighbours. Each MPR node maintains the list of knowing that were picked out as an MPR; this inclination is called as an MPR selector list. Only nodes selected MPR nodes are responsible for advertising well as sending on an MPR selector list advertised by other MPRs.

3. CASES OF ATTACKS FACED BY ROUTING PROTOCOLS

Due to their underlined architecture, ad-hoc networks are more easily attacked than a cabled net. The attacks prevalent on ad-hoc routing protocols can be broadly classified into passive and active attacks

A Passive Attack does not interrupt the performance of the protocol, but attempts to hear valuable data by taking heed to traffic. Passive attacks basically involve obtaining vital routing information by sniffing around the web. Such attempts are commonly difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to distinguish the precise placement of a node, one may be capable to find information about the mesh topology, using these attacks.

An Active Attack, however, injects arbitrary packets and tests to disrupt the performance of the protocol in order to limit availability, gain authentication, or attract packets destined to other odes. The finish is essentially to attract all packets to the attacker for analysis or to disable the network. Such attempts can be discovered and the lymph glands can be distinguished

In this report we try to examine some of the threats faced by the ad hoc network environment.

3.1 Blackhole attack

MANETs are vulnerable to several approaches. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function of the routing mechanism of the ad hoc network. In blackhole attack, the malicious node waits for the neighbours to initiate a RREQ (Request) packet. As the client receives the RREQ packet, it will forthwith transmit a false RREP (Reply) packet with a modified higher sequence number. Thus, that the source node assumes that the client is having the fresh route towards the address. The source node ignores the RREP packet received from other nodes and begins to broadcast the information packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects; data packets [10].

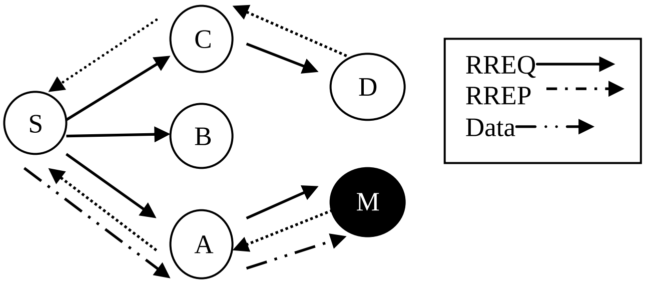


Fig 4. Blackhole Attack

In Fig 4, source node S wants to transmit data packets to a destination node D in the network. M node is a malicious node which works as a black mess. The attacker replies with a false reply RREP having higher modified.

3.2 Flooding Attack

The intention of the flooding attack is to beat the network resources, such as bandwidth and consume a node's resource, such as computational and battery power or to disrupt the routing procedure to cause severe degradation in network operation. For instance, in AODV protocol, a malicious node can broadcast a great number of RREQs in a short period to a destination node that does not exist in the mesh. Because no one will respond to the RREQs, these RREQs will flood the whole web. As a consequence, all of the node battery power, as well as network bandwidth will be eaten up and could contribute to denial-of-service. In [11], the authors establish that a flooding attack can decrease throughput by 84 percentages.

3.3 Link Withholding Attack

In this approach, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these clients. This character of approach is especially dangerous in the OLSR protocol.

3.4 Link Spoofing Attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbours to disrupt routing operations. For instance, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This makes the target client to select the malicious node to be its MPR. As an MPR node, a malicious node can then fake the data or routing traffic, for model, altering or dropping the routing traffic or doing other types of Denial of Service attacks.

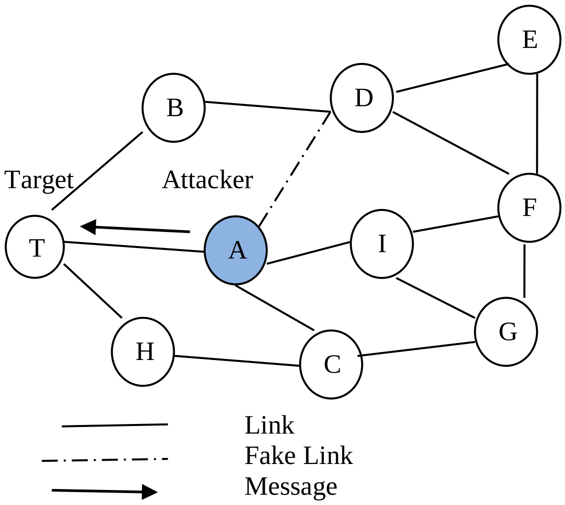


Fig 4. Link Spoofing Attack

The above Fig 4 shows an example of the link spoofing attack in an OLSR MANET. In this form, we take that node A is the attacking node, and node T is the prey to be set on. Before the attack, both nodes A and B are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbours. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node.

3.5 Replay Attack

In a MANET, topology frequently changes due to node mobility. This means that the current network topology might not exist in the future. In a replay attack [12], a node records another node's valid control messages and resend them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific client or simply to disturb the routing operation in a MANET.

3.6 Wormhole attack

A Wormhole attack [12] is one of the most advanced and severe attacks in MANETs. In this attack, a pair of colluding attacker's record packets at one location and replays them at another position using a private high speed web. The sincerity of this approach is that it can be set up against all communications that offer authenticity and confidentiality.

The following Fig 5 presents an example of the wormhole attack against a reactive routing protocol. In this figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the approach, when source node S broadcasts a RREQ to find a path to a destination node D, its neighbors J and K forward the RREQ as usual. However, node A1, which received the RREQ forwarded by node J, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ to its neighbor P. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Thus, node D will choose route D-P-J-S to unicast a RREP to the source node S and ignore the same RREQ that arrived later.

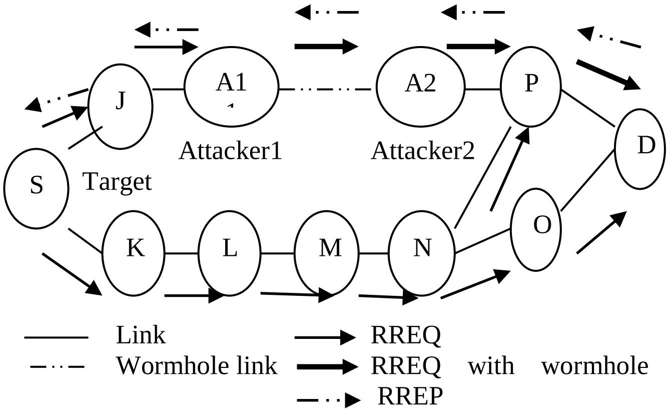


Fig 5. Wormhole Attack

As a result, S will select route S-J-P-D that indeed passed through A1 and A2 to send its data.

3.7 Colluding Misrelay Attack

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This approach is hard to detect by using the conventional methods such as watchdog and portraiture [13]. Fig 6 presents an example of this approach. Take the case where node A1 forwards routes packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. Nevertheless, the second attacker A2 drops or modifies these routing packets. In [14] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

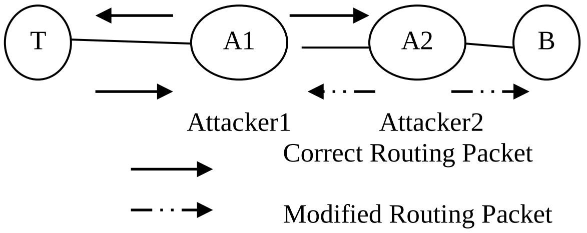


Fig 6. Colluding Misrelay Attack

4. ANALYSIS REPORT

Since there is no set up infrastructure in Ad hoc network, Security is a major topic. As MANETs typically lacks a fundamental authority for authentication and key distribution, security mechanisms must be scalable and capable of frequent topology changes. The trust element is an significant concept in network security, as it is the set of relations among agents participating in the network activities.

Cryptography is the technique utilized to provide data communication, security, integrity, authenticity, confidentiality and non-renunciation. The cryptographic system is separated into symmetric and asymmetric cases. The Symmetric system requires less processing than asymmetric, but clients should share the secret keys by a secure channel. In MANETs, there is no any pre-established channel. Hence, Symmetric system is not suitable for MANETs[15]. Whereas Asymmetric system requires a trusted entity to process key authentication and credential.

Cryptographic algorithms require public and private keys. The key management system is used to administrate these keys. It offers several processes like key generation, maintenance, distribution, protection, revocation of keys and ensures availability to clients. Identity-based coding is one of the key management strategies. Identity-based Cryptography is a pattern of asymmetric cryptography, which is appropriate for MANET. In this method, third party server uses a simple identifier such as email address, for generating public key. In identity-based cryptography, verification of user‟s validity is achieved by its unique identifier (ID). Private Key generates from a key generation center (KGC) while the Public Key is obtained from the user’s ID [16]. It is most suited for the MANET environment. We proposed Identity based cryptography to handle attacks in MANETs.

5. CONCLUSION

The development of MANET cannot be separated from the universe of computing. Since it is portable and compact media with which we can communicate exclusive of a wired network. In this review paper, we discussed some typical and dangerous vulnerability in the MANET, attack type security criteria and proposed Identity based cryptography, which move on to guide to the security-related research works in this area.

ACKNOWLEDGEMENT

My earnest thanks to my honorable Principal Rev. Fr. Dr. Antony Samy SJ, and Secretary Rev. Fr. Susaimanickam, Ananda College, Devakottai who are encouraging me for doing Research.

My heartfelt thanks honorable guide Dr. M. Ganaga Durga Assistant Professor, Govt. Arts College For Women, Sivagangai who contributed and supported towards the preparation of the paper.

REFERENCES

[1] Wireless World Research Forum (WWRF): http:// www.ist-wsi.org.

[2] S. Ci et al., “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,” IEEE Trans. Vehic.Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

[3] James A. Freebersyser, Barry Leiner, A DoD perspective on mobile ad hoc networks” Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.

[4] W. Fifer, F. Bruno, The low-cost packet radio, Proceedings of the IEEE 75 (1) (1987) 33–42

[5] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," Proc. ACM SIGCOMM '94, Oct. 1994.

[6] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," Proc. ACM Mobicom '94,

[7] M. Abolhasan, T. Wysocki, E. Dutkiewicz, ― A Review of Routing Protocols for Mobile Ad- Hoc Networks,Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003. Conference (ACMSE’04), pp. 96-97, Apr. 2004.

[8] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On-demand Distance Vector (AODV) Routing,” IETF RFC3561, July 2003.

[9] Th. Clausen et al., “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.

[10] Dokurer, Semih.”Simulation of Black hole attack in wireless Ad-hoc networks”. Master's thesis, AtılımUniversity, September 2006

[11] S.Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[12] Y-C. Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[13] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th MobiCom, Boston, MA, Aug. 2000.

[14] International Journal of Computer Science Engineering Research and Development (IJCSERD), ISSN 2248 – 9363 Volume 3, (2013), pp: 01-11 MANET– CHALLENGES, SECURITY AND PROTOCOLS Vikram m. Agrawal

[15] I.Chlamtac,M.Conti,and J.J.N.Liu, “Mobile ad hoc networking: imperatives and challenges,” AdHoc Networks, vol.1, no 1,pp. 13–64,2003.

[16] C. Yu, Y. Mu, and S. Willy, “An identity-based broadcast encryption scheme for mobile ad hoc networks”, Journal of Telecommunication and Information Technology, vol. 1, pp. 24-29, 2006.

[17] C. Sreedhar et al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 224-232 “A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols “

[18] IJCSI International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online): 1694-0784 ISSN (PRINTED): 1694-0814 DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET AYAL N. RAJ, PRASHANT B. SWADAS

[19] I. J. Computer Network and Information Security, 2013, 5, 64-72 Published Online April 2013 in MECS (http://www.mecs-press.org/) Effect of Black Hole Attack on MANET Routing Protocols Jaspal Kumar, M. Kulkarni, Daya Gupta

[20] Study of different types of attacks on multicast in mobile ad hoc networks Hoang Lan Nguyen, Uyen Trang Nguyen Department of Computer Science and Engineering, York University, Toronto, Ont., Canada M3J 1P3 Ad Hoc Networks 6 (2008) 32–46 www.elsevier.com

[21] IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009 MANET Security Issues Nishu Garg, R.P.Mahapatra

[22] Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks Hassen Redwan and Ki-Hyung Kim 2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology

[23] Volume 3, Issue 6, June 2013ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Security Issues in Manet: A Survey on Attacks and Defense Mechanisms Tarunpreet Bhatia A.K.Verma .