International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 12 4041 - 4046

Survey on EAACK- A Secure Intrusion - Detection System for MANETs

Priyanka D. Lohar
Computer dept.
JSPM'S BSIOTR (W)
Pune, India
e-mail: priyanka_lohar@live.com

Prof. Archana C. Lomte
Computer dept.
JSPM'S BSIOTR (W)
Pune, India
archanalomte@gmail.com

***Abstract*—** From the past few years' migration to wireless network from wired network has been a global trend. Wireless network made it possible in many applications to have mobility and scalability. Among all the modern wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. MANET is more popular now days. On the conflicting to traditional network architecture, MANET not has a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes within same communication range are communicated directly with each other. Otherwise, they depend on their neighbors to relay messages. Because of the self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. Now days, security has become a very important service in Mobile Adhoc Network. As Compared with other networks, MANETs are more vulnerable to various types of attacks. This paper presents an overview of Secure Intrusion-Detection Systems for discovering malicious nodes and attacks on MANETs. Because of some special characteristics of MANETs, prevention mechanisms alone are not satisfied to manage the secure networks. In this, detection should be focused as another part before an attacker can damage the structure of the system. This paper gives an overall overview of IDS architecture for improving the security level of MANETs. For enhancing the security based on security attributes and then various algorithms like RSA and DSA.

Keywords- *Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET).*

*****

I. INTRODUCTION

Wireless networking is very emerging concept nowadays, used in many real time applications. In recent manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are smaller, and so increasingly mobile. Mobile ad hoc networks i.e. MANETs combine wireless communication with a high degree of node mobility. Within a restricted range wireless communication and high node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. The powerful nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile situations. MANETs have thus become a very popular research topic and have been proposed for use in many areas such as rescue operations, tactical operations, environmental monitoring, conferences, and the like.

MANETs because of their very nature more vulnerable to attack than wired networks. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and computational capacities, and run usually on battery power) introduces new security risks. As part of rational risk management we must be able to identify these risks and take appropriate action. In some instance we may be able to design out particular risks cost-effectively. In other instance we may have to accept that vulnerabilities exist and seek to take appropriate action when we believe someone is attacking us. As a result, intrusion detection is an indispensable part of security for MANETs. Many intrusion detection systems (IDS) have been proposed in the literature for wired networks but MANETs' specific features make direct application of these approaches to MANETs impossible. For the MANETs has new approaches need to be developed or else existing approaches need to be adapted. In this chapter, we examine special IDS issues of MANETs and proposed IDSs for MANET-specific systems to find out how well proposed systems address these issues. In the next section, an introduction to intrusion detection systems is given. Then, intrusion detection on MANETs is discussed along with proposed IDSs. In conclusion, thoughts for practitioners and ideas for future research are given. The Mobile Ad hoc Wireless Network is more vulnerable to be attacked than wired network. These vulnerabilities are nature of the MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised to exploit these vulnerabilities and to cripple the MANET operation. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. The rest of this chapter is organized as follows – initially a classification of

 ISSN: 2321-8169
4041 - 4046

wireless networks in use today is described followed by the background and origins of ad hoc wireless networks. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting applications. A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a Fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. A MANET with the characteristics described above was originally developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. In recent years, MANETs have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where lap- tops, PDA or other mobile devices share wireless medium and communicate to each other. As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Therefore, only one compromised node can cause the failure of the entire network. There are both passive and active attacks in MANETs. For passive at- tacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication were Ø brought into consideration, and many techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in. Intrusion detection can be developed as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity.

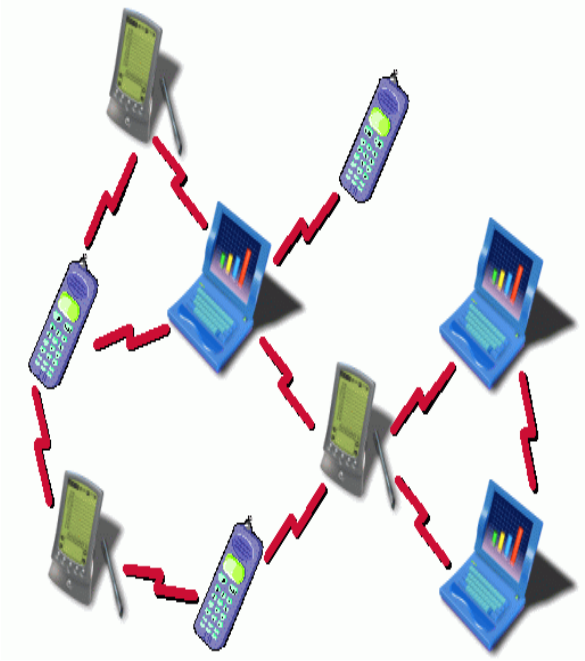

Fig.1. Mobile AdHoc Network

II. RELATED WORK

Intrusion detection is defined as the technique to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource”. For MANETs, the general function of IDS is to detect misbehaviors by observing the networks traffic in a Mobile Ad hoc. There are two important models of Intrusion detection systems namely signature based and anomaly based approaches [5] [6]. A signature-based IDS monitors activities on the networks and compares them with known attacks. However, a drawback of this approach is that new unknown threats cannot be detected. In anomaly-based detection, profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically and significantly different from what was determined to be normal, is flagged as suspicious. Anomaly detection can detect unknown attacks, But the issue is that anomaly based approaches yield high false positives for a wired network. If these statistical approaches are applied to MANET, the false positive problem will be worse because of the unpredictable topology changes due to node mobility in MANETs. The specification based approach, is recently presented and is ideal for new environments, such as

 ISSN: 2321-8169
4041 - 4046

MANETs. In specification-based detection, the correct behaviors of critical objects are abstracted and crafted as security specifications, which are compared to the actual behavior of the objects. Intrusions, which usually cause an object to behave in an incorrect manner, can be detected without exact knowledge about the nature of the Intrusions. Currently, specification-based detection has been applied to privileged programs, applications, and several network protocols. Most of recent researches focused on providing preventive schemes to secure routing in MANETs [10-14]. Security is most important service in MANETs

A Security attributes

Security has become a most important service in Mobile Adhoc Network (MANETs)[12]. Zhou and Haas have proposed using threshold cryptography for providing security to the network. To secure an ad hoc network, the following attributes are to be considered: availability, authentication and key management, confidentiality, integrity, non-repudiation, and scalability. In order to achieve this goal, the security solutions for each layer which are providing complete protection for MANETs are to be described.

There are five main layers on the network, as follows:

1. Application layer: Detecting and preventing viruses, worms, malicious codes.
2. Transport layer: Authenticating and securing end-to-end communication through data encryption.
3. Network layer: Protecting the ad hoc routing and forwarding protocols.
4. Link layer: Protecting the wireless MAC protocol and providing link-layer security support.
5. Physical layer: Preventing signal jamming denial-of-service attacks.

B Discovering malicious nodes

1) Watchdog: It is very popular and highly efficient IDS for improving the throughput of network with the presence of malicious nodes. This IDS can be classified into two methods such as Watchdog and Path rater. It is responsible for discovering malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by listening to its next hop's transmission in the network. If a Watchdog IDS overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold value, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

2) TWOACK: It is another important IDS TWOACK for discovering malicious nodes in MANETs [6]. The main aim of this ID to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

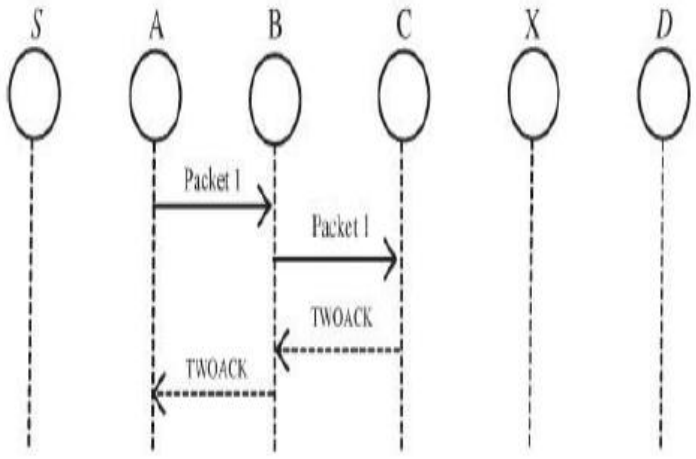

Fig: 2 TWO ACK IDS FOR MANETs

In Fig. 2: Node X wants to transmit the Packet 1 to node Y, and then, node Y transmit the Packet 1 to node Z. When node Z receives Packet 1, as it is two hops away from node X, node Z is generate a TWOACK packet, which contains reverse route from node X to node Z, and sends it back to node X. The retrieval of this TWOACK packet at node X indicates that the transmission of Packet 1 from node X to node Z is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes Y and Z are reported malicious. The same process applies to every three consecutive nodes along the rest of the route. The TWOACK IDS effectively processes the receiver collision and limited transmission power problems indicated by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problem [9].

3) AACK: It i1s same as TWOACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an ID called TACK (identical to TWOACK) and an end-to-end acknowledgment IDS called Acknowledge

 ISSN: 2321-8169
4041 - 4046

(ACK). Compared to TWOACK IDS, AACK IDS reduced network overhead. The end-to-end ACK IDS is shown in Fig. 3. The source node A sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node B receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node A along the reverse order of the same path. Within a predefined time slot, if the source node A receives this ACK packet, then the packet transmission from node A to node B is successful. Otherwise, the source node A will switch to TACK IDS by sending out a TACK packet. The concept of adopting a hybrid IDS in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and fake ACK packets.

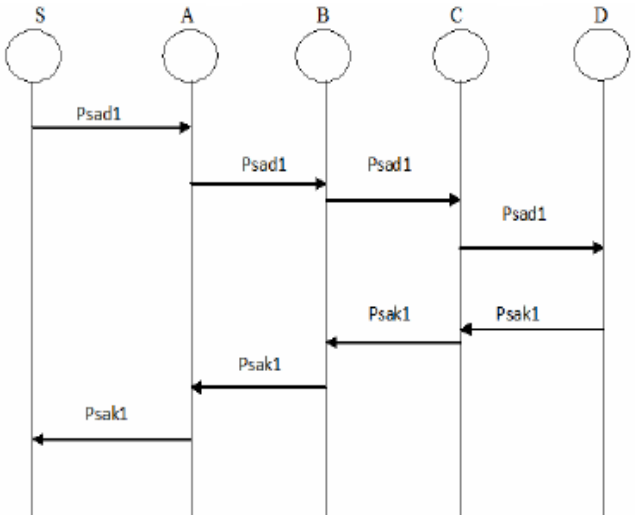

Fig: 3 END-END ACK for MANETs

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the ACK packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, a digital signature is adopted in recent secure IDS named Enhanced AACK (EAACK).

III. METHODOLOGY

Secure IDS architecture (EAACK) introduced to improve the security level of MANETs based on security attributes and various algorithms, namely RSA and DSA. EAACK is designed to tackle three out of six weaknesses of Watchdog IDS, namely, 1) Receiver collision, 2) Limited transmission power, 3) False misbehavior.

1) *Receiver collisions:* Example of receiver collisions, shown in Fig. 4, after node A sends Packet 1 to node

B, it tries to overhear if node Y forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node Y has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

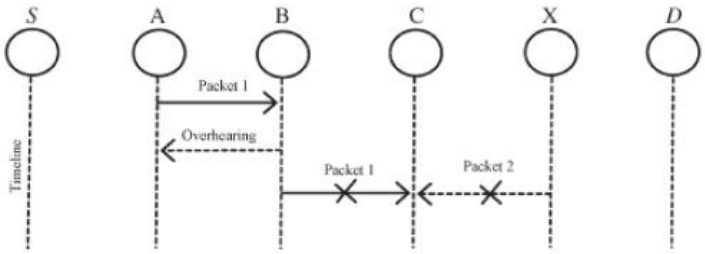

Fig: 4 receiver collision

2) Limited transmission power: Example of Limited power, shown in Fig. 5, in order to manage the battery resources in MANETs, node B limits its transmission power so it is very strong to be overheard by node X after transmitting the packet (P1) to node C , but too weak to reach node C because of transmission power can b reduced.

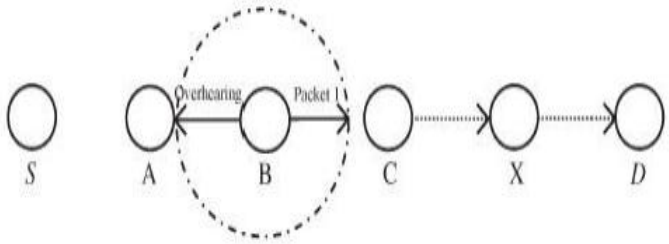

Fig: 5 limited transmission power

3) False misbehavior: Example of false misbehavior in MANETs, shown in Fig. 6, Even though node A and B forwarded Packet 1 to node C successfully, node A still inform node B as misbehaving, as shown in Fig. 6. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In order to solves not only receiver collision and limited transmission power but also the false misbehavior problem to launch Secure IDS architecture (EAACK) [1].

 ISSN: 2321-8169
4041 - 4046

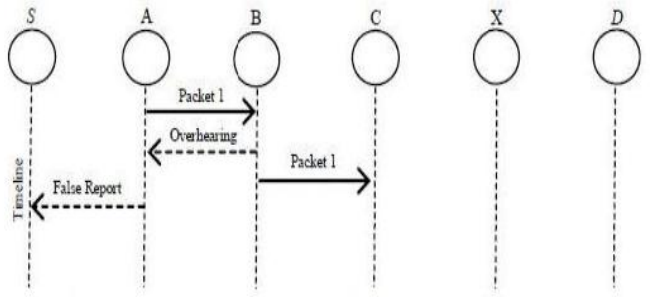

Fig: 6 false misbehavior

A Secure IDS description

EAACK is consist of three major components , namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes to include a 2-b packet header in EAACK. According to the Internet draft of DSR [7], there is 6 b reserved in the DSR header. In EAACK, use 2 b of the 6 b to flag different types of packets.

DATA	ACK	SACK	MRA

Fig. 7 EAACK protocol in MANETs

In these secure IDS, It is assumed that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

1) ACK: ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Consider the scenario source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

2) S-ACK: It is an improved version of the TWOACK IDS [6]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

3) MRA: Unlike the TWOACK IDS, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior. The MRA field is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA field is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

4) Digital Signature: EAACK is an acknowledgment-base IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on ACK packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. To overcome this problem, need to incorporate digital signature in secure IDS. In order to ensure the integrity of the IDS, EAACK requires all ACK packets to be digitally signed before they are sent out and verified until they are accepted [1].

B Secure IDS in DSA and RSA

The signature size of DSA is much smaller than the signature size of RSA. So the DSA scheme always produces slightly less network overhead than RSA does. However, it is interesting to observe that the Routing Overhead differences between RSA and DSA schemes vary with different numbers of malicious nodes [16]. The more malicious nodes there are, the more ROs the RSA scheme produces. Assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the

whole network overhead. With respect to this result, find DSA as a more desirable digital signature scheme in MANETs [1]. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.

IV. CONCLUSION

This paper gives a survey on various techniques of IDS. This Paper focuses on a comparative study of Secure Intrusion-Detection Systems (SIDS) for discovering malicious nodes and attacks on MANET. MANET having some special characteristics so prevention mechanisms alone are not satisfied to manage the secure networks. In this special attention on system as another part before an attacker can damage the structure of the system. This paper focused on the study about secure IDS named EAACK protocol specially designed for MANETs. Security is one of the important in MANETS, hybrid cryptography architecture will solve the issue in an efficient manner. Because of this way we can better preserve battery life and memory space of mobile nodes.

ACKNOWLEDGMENT

Authors thanks BSIOTR(W), Pune for every support to write this paper. Authors also acknowledge other contributors for their contribution in preparing such paper.

REFERENCES

[1] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, *IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE*

[2] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan, Ali Movaghar and Faroukh Koroupi, World Academic of Science Engineering and Technology 44 2008.

[3] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999, [4] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad,2009."Chapter 30: Security in wireless ad- hoc networks, the handbook of Ad hoc wireless network". CRC PRESS Publisher

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

[5] "A study of different types of attacks on multicast in mobile ad hoc networks" Hoang Lan Nguyen, Uyen Trang Nguyen, Elsevier AdHoc Networks(2008) 32-46.

[6] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[7] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[8] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in *Proc. 2nd Conf. m-Bus.*, Vienna, Austria, Jun. 2010

[9] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

[10] "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol"Ahmed M. Abdulla, Imane A. Saroitb, Amira Kotbb, Ali H. Afsaric a* 2010 Published by Elsevier Ltd.

[11] http://www.scribd.com/doc/55488795/48/MANETSecurity- Services#outer_page_29

[12] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks:Challenges and solutions" (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[13] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[14] "Security Issues in Mobile Adhoc Networks-A Survey" Wenjia Li and Anupam Joshi University of Maryland, Baltimore Country.

[15] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc.ACM Workshop Wireless Secur.*, 2002, pp. 1–10.

[16] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[17] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535– 541.