A Comparative Study of Secure Intrusion-Detection Systems for Discovering Malicious Nodes on MANETs

Rajeshkumar.G
Research Scholar & Assistant Professor (Senior Grade), Department of IT,
Velalar College of Engineering and Technology

K.R.Valluvan, PhD.
Professor and Head, Department of Electronics and Communications Engineering,
Velalar College of Engineering and Technology

ABSTRACT
In recent years, security has become a most important service in Mobile Adhoc Network. Compared to other networks, MANETs are more vulnerable to various types of attacks. In this paper, a comparative study of Secure Intrusion-Detection Systems for discovering malicious nodes and attacks on MANETs are presented. Due to some special characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of the system. First this paper gives an overview of IDS architecture for enhancing security level of MANETs based on security attributes and various algorithms, namely RSA and DSA. Then a hybrid cryptography IDS to further reduce the network overhead caused by digital signature is indicated.

General Terms
IDS architecture, RSA and DSA algorithm, Hybrid cryptography IDS.

Keywords
Mobile Adhoc Networks (MANETs), Secure Intrusion-Detection Systems (SIDS), malicious nodes.

1. INTRODUCTION
Mobile Adhoc Network (MANET) is collection of wireless mobile hosts (or nodes) that are free to in any directions at any speed. Mobile nodes are equipped with a wireless transmitter and a receiver that communicate directly with each other or forward message through other nodes.

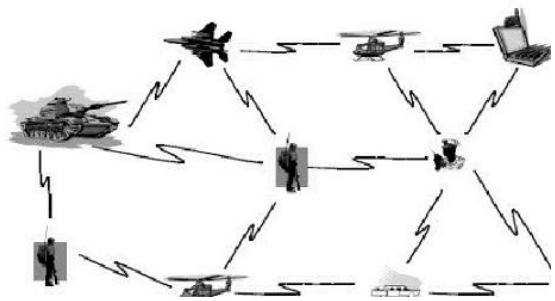

Fig. 1 Mobile Adhoc Network

One of the major advantages of mobile networks is to allow different nodes for data communications and still maintain their mobility. However, this communication is limited to the range of transmitters. It means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate nodes to relay data transmissions. This is achieved by dividing MANET into two types of networks such as single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. But in a multihop network, nodes rely on other intermediate nodes to transmit if the end point node is out of their radio communication range [1]. MANET is capable of operating a self-maintaining and self-organizing network without the support of any fixed infrastructure. MANET does not require expensive base stations of infrastructure dependent network (single-hop wireless networks). As MANETs have different characteristics from wired networks and even from single-hop wireless networks, there are more number of new challenges interrelated to security issues that need to be addressed. Initially, MANET was designed for military applications, but, in recent years, has found new usage. For example, search and rescue mission, data collection, virtual classes and conferences where laptops, PDA or other mobile devices are in wireless communication. Since MANET is being used wide spread, security has become a very important issue [2]. In general, MANETs are vulnerable based on the basic characteristics such as open medium, changing topology, absence of infrastructure, restricted power supply, and scalability. In such case, Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System (IDS) [2] [3].

The rest of the article is organized as follows. Section 2 presents the review of about SIDS in MANETs. Section 3 presents the IDS architecture for enhancing security level of MANETs based on security attributes and various algorithms, namely RSA and DSA. Finally, conclusion and discussion are presented in Section 4

2. REVIEW OF SIDS IN MANETs
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 misbehaviours 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 behaviour 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 MANETs. In specification-based detection, the correct behaviours of critical objects are abstracted and crafted as security specifications, which are compared to the actual behaviour 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.

2.1 Security attributes

Security has become a most important service in Mobile Adhoc Network (MANETs). 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, and application abuses.
2. Transport layer: Authenticating and securing end-to-end communications 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.

Table 1. Security attributes in MANETs

S.No	Attributes	Goals	Method
1	Availability	Resources can be accessed by all the nodes with in this network.	Distributed Adaptive Service Replication (DAR)
2	Authentication and key management	It ensures that data transmission is authentic.	Hybrid cryptography technique.
3	Confidentiality	It protects data from unauthorized person.	Converting original data into an unintelligible format using Data Encryption Standard(DES)
4	Integrity	It ensures that data being transmitted is never corrupted.	Cryptographic hash function algorithm
5	Non-repudiation	It ensures that sending and receiving information among all the nodes with in this network	Digital signature
6	Scalability	It ensures that newly added nodes in the network to be managed without any corruption.	Secure routing protocols used to manage the scalability.

2.2 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 Pathrater. It is responsible for discovering malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours 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 Pathrater 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 misbehaviour 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 IDS 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).

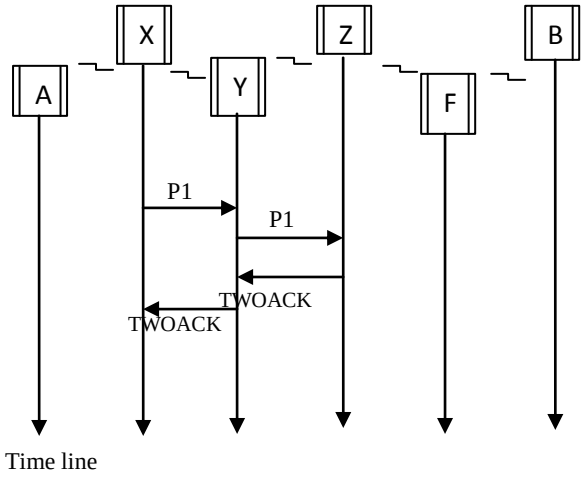

Fig. 2 TWOACK IDS for MANETs

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.

*3) AACK***:** It is same *as* TWOACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an IDS called TACK (identical to TWOACK) and an end-to-end acknowledgment IDS called ACKnowledge (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 misbehaviour report and fake ACK packets.

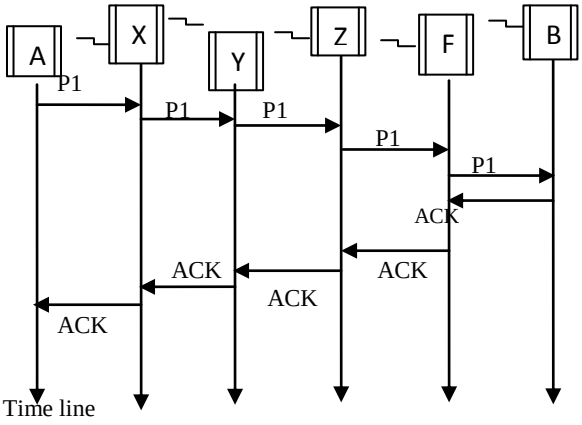

Fig. 3 End-to-End ACK IDS for MANETs

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).

3. A RECENT SECURE IDS ARCHITECTURE

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 misbehaviour.

1) Receiver collisions: Example of receiver collisions, shown in Fig. 4, after node X sends Packet 1 to node Y, it tries to overhear if node Y forwarded this packet to node Z; meanwhile, node F is forwarding Packet 2 to node Z. In such case, node X overhears that node Y has successfully forwarded Packet 1 to node Z but failed to detect that node Z did not receive this packet due to a collision between Packet 1 and Packet 2 at node Z.

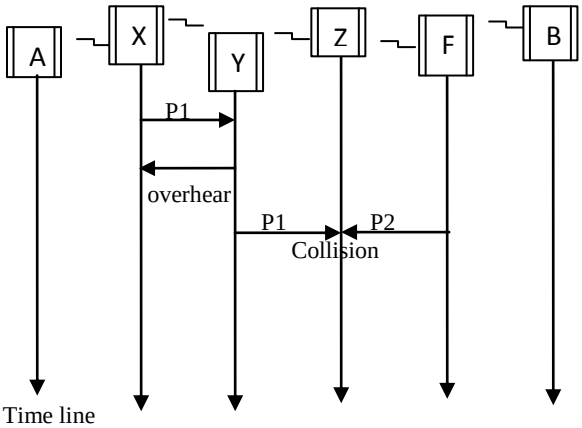

Fig. 4 Receiver collisions in MANETs

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

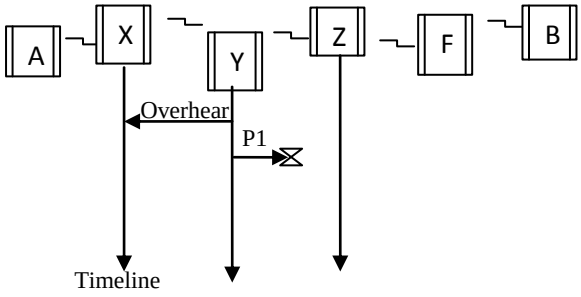

Fig. 5 Limited transmission power in MANETs

*3) False misbehaviour***:** Example of false misbehaviour in MANETs, shown in Fig. 6, Even though node X and Y forwarded Packet 1 to node Z successfully, node X still inform node Y 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 misbehaviour 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 misbehaviour attack. In order to solves not only receiver collision and limited transmission power but also the false misbehaviour problem to launch Secure IDS architecture (EAACK) [11].

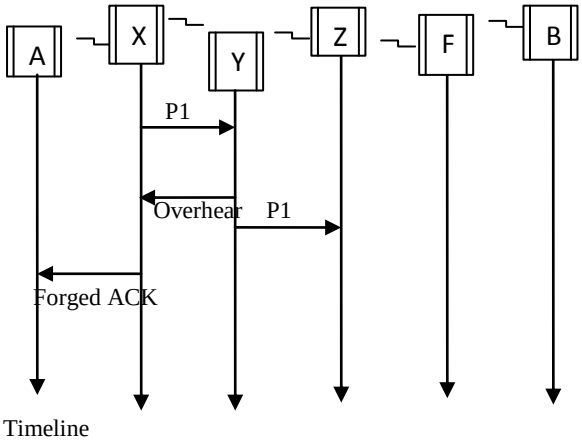

Fig. 6 False misbehaviour in MANETs

3.1 Secure IDS description

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour 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	S-ACK	MRA

Fig. 7 EAACK protocol in MANETs

In this 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 misbehaviour 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 misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour.

The MRA field is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour. The false misbehaviour 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 misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

4*) Digital Signature:* EAACK is an acknowledgment-based 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 misbehaviours 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].

3.2 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. 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.

4. CONCLUSION AND FUTURE DIRECTIONS

In this survey paper, a comparative study of Secure Intrusion-Detection Systems (SIDS) for discovering malicious nodes and attacks on MANETs is presented. Due to some special characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of the system.we study about secure IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehaviour report. As security is major part in MANETS, hybrid cryptography architecture will tackle the issue in an efficient manner.

5. ACKNOWLEDGMENTS

I give my sincere feelings of thankfulness to Dr. K.R.Valluvan for his valuable guidance, support and encouragement which helped me a lot to write this paper. And also I would like to grateful the anonymous reviewers for their comments and suggestions that helped to improve the quality of the article.

6. 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,2003."Chapter 30:Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network". CRC PRESS Publisher

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

[6] "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. [7] 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.

[8] 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.

[9] 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. 2003.

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

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

[12] http://www.scribd.com/doc/55488795/48/MANET-Security-Services#outer_page_29

[13] 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.

[14] 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.

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

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

[17] 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.

[18] 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.

[19] Karan Singh, R. S. Yadav, Ranvijay, "A REVIEW PAPER ON AD HOC NETWORK SECURITY",International Journal of Computer Science and Security, Volume (1): Issue (1)