Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.385 – 392

REVIEW ARTICLE

REVIEW PAPER ON RESPONSE BASED APPROACHES FOR DETECTION OF MISBEHAVING NODES IN MANETS

Swapna Taksande[1], Prof. Rajani Bhoomarker[2], Prof. Sameena Jafar[3]

[1]Department of Electronics and Communication, Rajeev Gandhi Proudyogiki Vishwviyalaya, India
[2]Department of Electronics and Communication, Rajeev Gandhi Proudyogiki Vishwviyalaya, India
[3]Department of Electronics and Communication, Rajeev Gandhi Proudyogiki Vishwviyalaya, India
[1] swapna.t2007@gmail.com, [2] jounjarerajni@gmail.com,[3] hodecpatelcollege@gmail.com

Abstract: **Mobile Ad-hoc Networks (MANET) are Infrastructure less networks where self-configuring mobile nodes are connected by wireless links. In MANET, each node in a network performs as both a transmitter and a receiver. They rely on each other to store and forward packets. Due to inherent characteristics like decentralization, self configuring, self -organizing networks, they can be deployed easily without need of expensive infrastructure and have wide range of military to civilian and commercial applications. But wireless medium, dynamically changing topology, limited battery and lack of centralized control in MANETs, make them vulnerable to various types of attacks. Intrusion Detection System (IDS) is required to detect the malicious attackers before they can accomplish any significant damages to the network. This paper focus on problem of misbehaving nodes in MANETs which is based on Dynamic source routing. As well as for above said problem this papers point out pros and cons of various responses based techniques.**

Keywords- MANET; Misbehaving nodes; DSR; Selfish nodes; forged acknowledgement

I.INTRODUCTION

A Mobile Ad hoc Network, or MANET, consists of a group of cooperating wireless mobile hosts (nodes) that dynamically constructs a short lived and self-configuring network without the support of a centralized network infrastructure. The mobile nodes can be cell-phones, PDAs and laptops and typically support several forms of wireless connectivity like 802.11, IrDA, Bluetooth, etc. MANETs have number of applications like in military where nodes are scattered on battlefield for surveillance mission, in emergency and disaster struck areas where an infrastructure is unavailable or unfeasible to install and for ubiquitous computing for smart homes. MANETs are also used in mobile conferencing for business meetings and seminars involving a

© 2014, IJCSMC All Rights Reserved

large group of people where access points may be absent or inaccessible. Hence MANETs has wide range of military to civilian and commercial applications.

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks. But most of these schemes become worthless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defense line of network become ineffective.

Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect. There are two types of attacks in MANETs, namely: passive and active attacks. In passive attacks, packets containing secret information might be overhear, which violates confidentiality.

In active attacks, new nodes join and inject packets to invalid destinations into the network, which cause existing packets disjoin or dropped. Modifying the contents of packets and impersonating other nodes violates availability, integrity, privacy and confidentiality. [8]

Fig.1 Mobile ad hoc network

In this paper, we have chosen one of the reactive protocols, namely Dynamic Source Routing (DSR) protocol. The reason being, it uses source routing, (that is the packet header contains the path to be followed by the packet), as the source node need to know the identity of every intermediate node in the route to destination. It also avoids the need of constantly updating routing information in the intermediate nodes.

II.ROUTING PROTOCOLS IN AD HOC NETWORKS

In mobile ad hoc networks, due to the limited wireless transmission range, it is usually the case that paths between source nodes and destination nodes require multiple hops. In this case, every node may act as a router to forward packets from the source to the destination. Also, due to the nodes mobility, it is necessary to change the existing routes in order to maintain the connection between them. A MANET routing protocol must be able to quickly detect and respond to such state changes in order to minimize degradation in services provided to existing sessions.

There are many different routing protocols that can be used in MANET. In general, they can be classified into two main groups: proactive routing and reactive routing, depending on the time when route are determined. Proactive routing constantly formulates routing choices in order to have accessible paths available for nodes that need to send packets [7]. Reactive routing on the other hand only finds a route when requested; as soon as a node has a packet to transmit, it queries the network for a route.

III.DYNAMIC SOURCE ROUTING (DSR)

This protocol is referred to as "on-demand" because route paths are discovered at the time a source sends a packet to a destination for which the source has no path. The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. [22]

Route Discovery is the mechanism by which a node S wishing to send a packet to a destination D obtains a source route to D. To perform a Route Discovery, the source node S broadcasts a ROUTE REQUEST (RREQ) packet that is flooded through the network in a controlled manner. When the intermediate node receives the RREQ, it first adds its address to the RREQ, and then rebroadcasts the modified RREQ. When the destination node receives the RREQ, it constructs a RREP (Route Reply), and

© 2014, IJCSMC All Rights Reserved

copies the accumulated route in the RREQ to the RREP, and sends the RREP to the source on the reverse path. If intermediate node has route available to the destination node, it first adds this route to the RREQ, and then constructs a RREP, and sends the RREP to the source on the reverse path. At last, when the source receives the RREP, it knows there is a route to the destination node, and copies the route in the RREP to its memory for later use.
Route Maintenance mechanism indicates if a source route is broken or if the network topology has changed, such that it can no longer uses its route to the destination. Then S is notified with a ROUTE ERROR (RERR) packet. The sender S can then attempt to use any other route to D already in its cache or can invoke Route Discovery again to find a new route. In this paper we spotlight on various response based Detection and prevention technique for forged acknowledgement and misbehaving nodes in MANETs based on Dynamic source routing protocol.

IV.MISBEHAVING NODES IN MANETS

An individual mobile node may attempt to benefit from other nodes, but refuses to share its own resources. Such nodes are called selfish or misbehaving nodes, and their behavior is termed selfishness or misbehavior [12].

- A selfish or malicious node may agree on forwarding control packets while drop all or part of the data packets it received to conserve its energy. This type of attacks is termed as DoS or black hole attack[2]
- A malicious node may drop the packets, modify the routing information or impersonate other nodes with the intention to disrupt the network and affect its availability.
- A selfish node is unwilling to spend battery life, CPU cycles and available network bandwidth to forward packets [1].
- The malicious nodes are classified into two types: ordinary attackers and smart attackers. The main difference between the two types is that the smart attackers can do a receiver collision and limited transmission power [9].

In this paper we discuss response based techniques in which receiver of data packet confirms the reception by sending response acknowledgement back to sender.

V.LITERATURE SURVEY

1) Watchdog is the basis for many of the techniques that are proposed in this field. It is initially proposed by **Marti et al** in his paper **"Mitigating Routing Misbehavior in Mobile Ad hoc Networks**" published in 2000 [1]. A scheme that contains two major modules, termed watchdog and path rater, to detect and mitigate, respectively, routing misbehavior in MANETs. Nodes operate in a promiscuous mode wherein the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of recently sent packets. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog module accuses the next hop neighbor of misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level. Based on the watchdog's claim, the path rater module rates every path in its cache and afterward chooses the path that best avoids misbehaving nodes. The watchdog is based on passive feedback that is overhearing, to confirm whether next has forwarded the packet or not. So it has weaknesses, that it might not detect a misbehaving node in the presence of ambiguous collision, receiver collision, limited transmission power, false misbehavior reporting, collusion and partial dropping.

2) Other related works in this field is the one presented by **Nasser and Chen** in their paper "**Enhanced intrusion detection system for discovering malicious nodes in mobile ad-hoc networks**" [7]. In their work, they proposed an enhanced intrusion detection system for discovering malicious nodes in MANETs called ExWatchdog. ExWatchdog extends the Watchdog proposed in [1]. The study succeeds in solving one of the problems that were listed above in the weaknesses of the Watchdog technique, which is the false misbehaving problem, where a malicious node falsely reports other nodes as misbehaving while in fact it is the real intruder. A table is maintained by each node, this table records the number of packets the node sends, forwards or receives, respectively. When the source receives a report about misbehaving node, it will find another path to ask the destination node about the number of received packets. If it is equal to the packets that the source has sent, then the real malicious node is the node that reports other nodes as misbehaving. Otherwise, nodes being reported malicious do misbehave. However, there is a limitation in this technique. If the true misbehaving node is in the all available paths from source to destination, then it is impossible to confirm and check the number of packets with the destination.

© 2014, IJCSMC All Rights Reserved

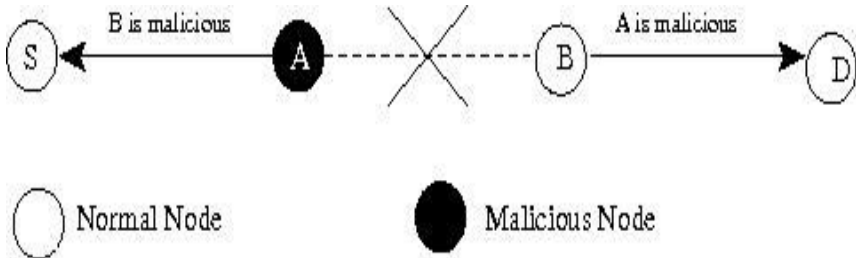

Fig.2 ExWatchdog Scheme

Above mentioned approaches are based on passive overhearing but there are other techniques which uses active feedback that is acknowledgement, for confirmation of the reception of data packets by a node which solves all the problems of Watch dog and Exwatchdog scheme.

3) **K. Balakrishnan et al** in their paper**"TWOACK: preventing selfishness in mobile ad hoc networks"** [5] proposed TWOACK scheme to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source to the destination. Suppose node A has discovered a route to node F with a source route A → B → C → D→E→F. In TWOACK, when node B forwards a packet to A, C (node C two hops away from A) receives the packet and sends an acknowledgement to node A indicating node B has forwarded the packet properly. If node A does not receive an acknowledgement for the packet that it expects to be forwarded by node B to node C within a certain timeout period, it suspects node B to be misbehaving. The same procedure is carried out by every set of three consecutive nodes along the source route. In TWOACK, each forwarded packet has to be recognized which may add to traffic congestion on the routing path.

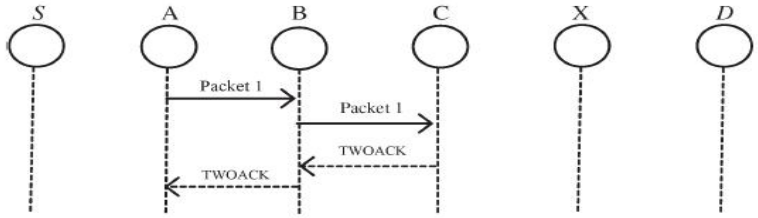

Fig.3 TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

K. Balakrishnan et al.[5] proposed S-TWOACK (Selective-TWOACK) scheme, a derivative of the TWOACK scheme, reduces this extra traffic due to TWOACK. In the S-TWOACK scheme, instead of sending back a TWOACK packet every time when a data packet is received, a node waits until a certain number of data packets (through the same triplet) arrive. The node then sends back one TWOACK packet acknowledging multiple data packets that have been received so far.

4) **K. Lui et al** in their paper **"An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs"** [4] proposed the 2ACK scheme which works like TWOACK with differences i) The data packet receiving node sends 2ACK packets as acknowledgment for a fraction of received data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead. 2) The 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine. The 2ACK scheme suffers from false misbehavior report.

5) Al-Roubaiey et. al.in their paper"**AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement"** [11] proposed Adaptive ACKnowledgment (AACK) scheme. The AACK is a network layer acknowledgment-

© 2014, IJCSMC All Rights Reserved

based scheme that may be considered as a combined system of an Enhanced-TWOACK (E-TWOACK), which detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead of TWOACK. The AACK mechanism may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitation will give the misbehaving nodes more time for dropping more packets. Also AACK still suffers from the partial dropping attacks (gray hole attacks). It also suffers from false misbehavior report. Further a misbehaving node may send fabricated acknowledgements.

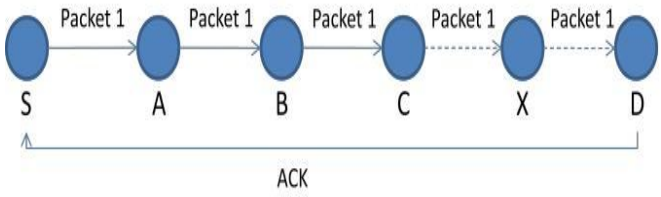

Fig. 4 ACK Scheme

6) N. Kang et. Al. in **"Detecting misbehaving nodes in MANETs"[**12] proposed Enhanced Adaptive ACKnowledgement (EAACK) scheme which consists of three parts (i) Acknowledge (ACK) (ii) Secure-ACKnowledgement (S-ACK) (iii) Misbehavior Report Authentication (MRA). ACK is basically an end-to-end acknowledgement scheme. In ACK mode if destination node D successfully receives data packet, it send back an ACK acknowledgement packet along the same route but in a reverse order. Within a predefined time period, if node S receives ACK, 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. S-ACK scheme is an improved version of TWOACK. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node as done in TWOACK. If the first node in a group does not receive S-ACK then it declare both second and third node as misbehaving nodes and send the report to source node. The source node do not immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. With MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

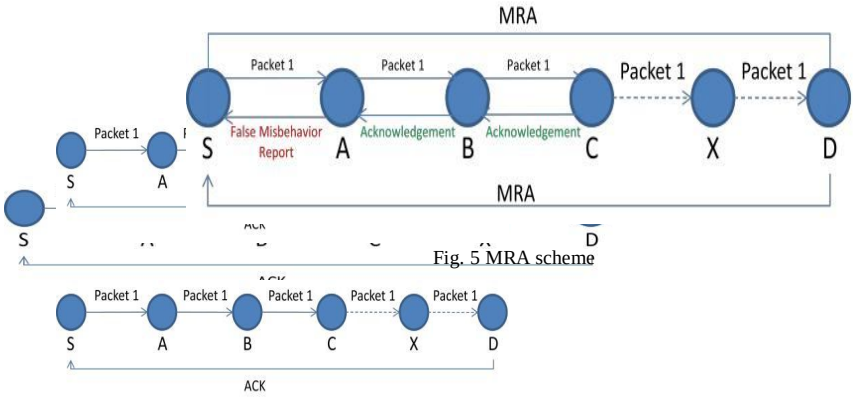

Fig. 5 MRA scheme

7) N. Kang, et. Al in **"Detecting Forged Acknowledgements in MANETs"** [14] proposed EAACK2; in this acknowledgement packets received in S-ACK phase of EAACK are digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet. Both the EAACK and EAACK2 cannot detect partial dropping that is Gray hole, during the first phase node may drop packets as end to end acknowledgement take time.

8) E.Shakshuki et.al in **"EAACK—A Secure Intrusion-Detection System for MANETs" [**18**]** proposed EAACK with the introduction of digital signature to prevent the attacker from forging acknowledgment packets.

© 2014, IJCSMC All Rights Reserved

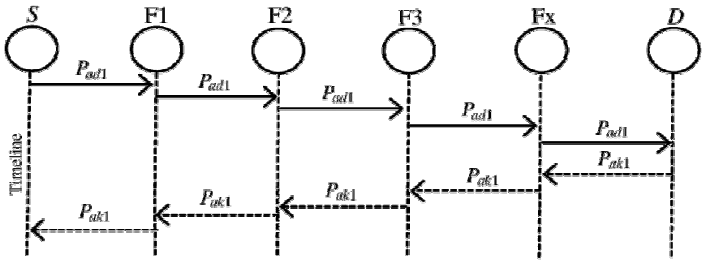

Fig. 6 System control flow: This figure shows the system flow of how the EAACK scheme works

EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA). In order to distinguish different packet types in different schemes, they included a two-bit packet header in EAACK. According to the Internet draft of DSR [22], there are six bits reserved in DSR header. In EAACK, two of the six bits were used to flag different type of packets. In the proposed scheme it was assumed that the link between each node in the network is bi-directional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.

VI.COMPARATIVE STUDY

Summarized comparison of above reviewed techniques is tabularized as follows:

TABLE 1. COMPARISON OF VARIOUS APPROACHES

S.N.	TITLE	EXTRACT OF THE PAPER	ROUTING OVERHEAD	DETECT FALSE MISBEHAVIOR REPORT	PREVENT ACKNOWLEDGEMENT FORGING	SOLVE RECEIVER COLLISIONS PROBLEM
1.	"TWOACK: preventing selfishness in mobile ad hoc networks"	TWOACK scheme to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source to the destination.	LARGE	NO	NO	YES
2.	An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs	The 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme	LESSER THAN TWOACK	NO	YES	YES
3.	AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement,	The AACK is a network layer acknowledgment based scheme, detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead of TWOACK.	LESSER THAN ABOVE TECHNIQUES	NO	NO	YES

© 2014, IJCSMC All Rights Reserved

4.	Detecting misbehaving nodes in MANETs	Enhanced Adaptive ACKnowledgement (EAACK) scheme which consists of three parts (i) Acknowledge (ACK) (ii) Secure ACKnowledgement (S-ACK) (iii) Misbehavior Report Authentication (MRA).	SAME AS AACK	YES	NO	YES
5.	Detecting Forged Acknowledgements in MANETs	Acknowledgement packets received in S-ACK phase of EAACK are digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet(EAACK2)	SAME AS EAACK	YES	YES	YES
6.	EAACK—A Secure Intrusion-Detection System for MANETs	The link between each node in the network is bi-directional, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.	SAME AS EAACK	YES	YES	YES

VII.CONCLUSION

Each scheme mentioned above except all EAACK techniques suffer from false misbehavior reports. Receiver collision problem is solved by all response based schemes. Future work is to comparatively analyze the simulations of reviewed techniques on basis of various parameters like routing overhead, end to end delay, energy consumption and packet delivery ratio.

ACKNOWLEDGMENT

First of all we want to thank the God Almighty for showering blessings on us in preparing this paper. Then we thank our family members. We thank our educators for guiding us. Last, but not least we thank all acquaintances for giving us support for doing this work.

REFERENCES

[1] S. Marti, T.J. Giuli, K. Lai, and M. Baker. "Mitigating Routing Misbehavior In Mobile Ad hoc Networks". In the *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ACM, pp. 255-265, Boston, Massachusetts, US, 2000.

[2] Animesh Patcha and Amitabh Mishra "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks" In: *Radio and Wireless Conference*, RAWCON '03, pp. 75–78 (2003).

[3] Parker, J., Undercoffer, J., Pinkston, J., Joshi, A. "On intrusion detection and response for mobile ad-hoc networks". In*: IEEE Inter- national Conference on Performance, Computing, and Communications*,pp. 747–752 (2004)

[4] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in *Proc. 3rd Int. Conf. Pervasive Comput. Commun.*, 2005, pp. 191–199.

[5] Balakrishnan, K.; Jing Deng; Varshney, V.K., 2005 "TWOACK: preventing selfishness in mobile ad hoc networks", In *Proceedings of Wireless Communications and Networking Conference*, 2005 IEEE , vol.4, no., pp.2137-2142(March 2005).

[6] Liu K., Deng J., Varshney P.K. and Balakrishnan K., 2007, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs". *IEEE Transactions on Mobile Computing*, May, 536-550.

[7] Nasser, N., Chen, Y. "Enhanced intrusion detection system for discovering malicious nodes in mobile ad-hoc networks", *IEEE International Conference on Communications*, ICC '07, pp. 1154–1159 (2007)

[8] T. Anantvalee and J. Wu. "A Survey on Intrusion Detection in Mobile Adhoc Networks", In *Wireless/Mobile Security*, Springer, 2008.

© 2014, IJCSMC All Rights Reserved

[9] Tanapat, A.:"On detection mechanisms and their performance for packet dropping attack in ad hoc network". *Dissertation, University of Pittsburgh* (2008).

[10] Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video Transmission enhancement in presence of misbehaving nodes in MANETs,"*Int. J. Multimedia Syst*., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[11] Al-Roubaiey A., Sheltami T., Mahumad A., Shakshuki E., Mouftah H, 2010 "AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement", *The 24th International Conference on Advanced Information Networking and Applications (AINA)*, IEEE Computer Society.

[12] Kang, N., Shakshuki, E and Sheltami, T., 2010." Detecting Misbehaving Nodes in MANETs", In *Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services* (iiWAS2010), ACM, pp. 216-222.

[13] Sagar Aishwarya., Ukey Anand & Chawla Menu, 2010 "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", *International Journal of Computer Science issues*, vol 7, Issue 4,No. 1, pp 12-17

[14] Kang, N., Shakshuki E and Sheltami T. 2011 "Detecting Forged Acknowledgements in MANETs", *The 25thInternational Conference on Advanced Information Networking and Applications (AINA)*, IEEE Computer Society, Biopolis, Singapore.

[15] Peyman Kabiri and Mehran Aghaei "Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks" *International Journal of Network Security*, vol.12, no.1, pp.42 {49, Jan. 2011.

[16] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks "in *journal of computing*, volume 3, issue 1, January 2011, issn 2151-9617.

[17] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in *Communications in Computer and Information Science*, Vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[18] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs", *IEEE transactions on Industrial electronics*, Vol. 60, No. 3 March 2013.

[19] U. Sharmila Begam, Dr. G. Murugaboopathi1 "A Recent Secure Intrusion Detection System for MANETs" *International Conference on Information Systems and Computing* (ICISC-2013),

[20] Umesh Prasad Rout "A Study of Intrusion Detection Systems in MANETs" *International Journal of Research in Computer and Communication Technology"*, Vol 2, Issue 2, Feb-2013.

[21] Treesa Nice P. A."A Survey on Intrusion Detection Systems in Mobile Ad Hoc Networks" *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 5, May 2013

[22] M. Zapata and N. Asokan. "Securing Ad hoc Routing Protocols". *In the ACM Workshop on Wireless Security*, pp. 1-10, 2002.

© 2014, IJCSMC All Rights Reserved