International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 1, pp: (97-102), Month: January - March 2015, Available at: www.researchpublish.com

EAACK—A Secure Intrusion-Detection System for MANETs

Kiran Shinde [1], Prof. Harjeet Kaur[2], Dr. Prakash Patil[3]

[1, 2, 3] Pune University, Indira College of engineering, Pune, India

Abstract: **Migration to wireless networks from wired network is global trends since last few years. Since the self configuration and without infrastructure in nature Manet is preferred in so many applications. Mobile Ad hoc network is a collection of wireless nodes forming a wireless network without infrastructure. In Manets all the nodes are communicating with each other via bidirectional links either directly or indirectly. Compared to other networks mobile Ad hoc network is more vulnerable to various types of attacks. A new intrusion detection system is designed for Manets by the adoption of MRA scheme named as enhanced adaptive acknowledgement (EAACK). EAACK is a capable of detecting maliciousness in the network also EAACK has overcome the attacks of watchdog, ACK and two ACK. In this paper the study of enhance security detection system for dissolving malicious nodes and attacks on mantes. Due to some special function of Manets only prevention is not good for managing the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of system.**

Keywords: **MANETS, DSA, RSA, EAACK, AACK, TWOACK, IDS, MRA, S-ACK.**

I. INTRODUCTION

Since the first day of invention wireless network is popular because of their scalability and natural quality. Because of their improved technology and reduced cost wireless network is used over wired network. Mobile ad hoc network is collection of mobile nodes which can move anywhere anytime. Mobile nodes equipped with both wireless transmitter and receiver communicates with each other. But this communication range is limited to transmitter range. That means two nodes cannot communicate with each other if the nodes are beyond the communication range. Manet solves this problem by allowing intermediate nodes for data transmission this achieved by dividing network in two types as single hope and multihope network. In single hope network the nodes can directly communicate with each other within the communication range. But in multihope network nodes are rely on intermediate nodes if the end node is not within the range of communication range [1]. Manet has different characteristic as compared to wired networks there are so many challenges related with security that need to be addressed. Initially Manet is designed for military applications but now days it is used for search and rescue mission and data collection, virtual class, and conferences where laptops, PDAs and other mobile phones are used. Since the wireless network is spreading the security is main issue in the wireless network. 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].

II. EXISTING SYSTEM

A. Intrusion detection in manets:

1) ***Watchdog:*** - The Watchdog is nothing but the combination of two elements, namely, Watchdog and Path rater. Watchdog detects malicious misbehaviors to its next hop's transmission. If a watchdog node Overhears that its next node fails to forward the packet among a particular amount of time, it will increase its failure counter. Whenever a node's failure counter exceeds a predefined threshold, 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 fails to observe malicious misbehaviours with the presence of the following:

1) Ambiguous collisions;

2) Receiver collisions;

3) Restricted transmission power;

4) False misbehaviour report;

5) Collusion; and

6) Partial dropping.

2. *Two ACK*: - with respect to six weaknesses in watch dog scheme several researches find out solution of these six weaknesses to solve these problems. TwoACK schemes detects the misbehaving links by acknowledging each information packet transmitted over each three consecutive nodes from source to destination it is another important IDS to detect malicious nodes in the manet [4]. The main aim of these IDS is to solve the receiver collision problem and limited power transmission problem of watchdog. After receiving the packet each node has to send acknowledge packet to the node that is two hopes away from it down the route. Two ACK is required to work on the routing protocol such as dynamic source routing (DSR).

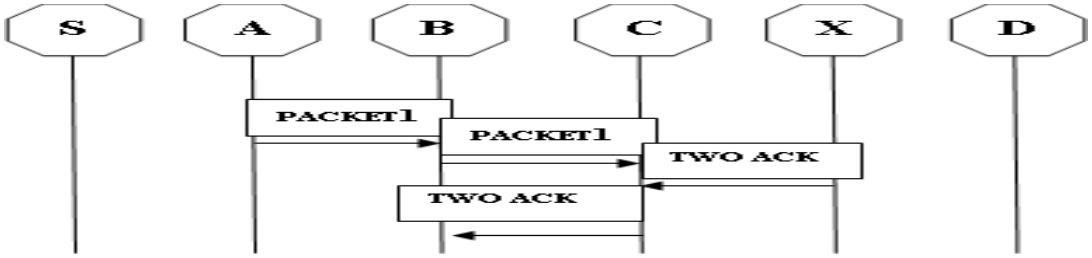

Fig.1 Two ACK

The operating method of TWOACK is shown in Fig. 1: Node A primary forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. Once node C receives Packet 1, because it is two hops from node A, node C should send TWOACK packet, that contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of packet one from node A to node C is fortunate. Otherwise, if this TWOACK packet is not received in an exceedingly predefined period, each nodes B and C area unit reported malicious. Identical method applies to each three consecutive nodes on the remainder of the route. However the acknowledgement process in every packet the unwanted overhead is added in every packet due to limited power nature of Manets. Such process will degrade the life span of entire network.

3. *AACK:* - Adaptive acknowledgement (AACK) is same as the two acknowledgements the difference is only that it provide end to end acknowledgement. As compared with two acknowledgements it reduces the network overhead still provides the identical network output.

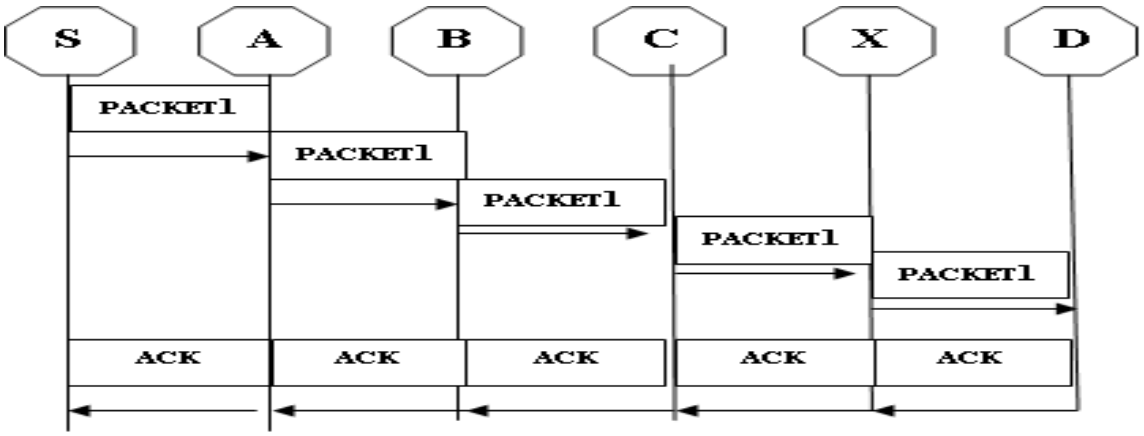

Fig.2 AACK

The end-to-end ACK IDS is shown in Fig. 2. The source node S sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same path. Within a predefined time slot, if the source node S receives this ACK packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK (TWO ACK) 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

III. PROBLEM DEFINATION

(EAACK) i.e. Enhanced Adaptive Acknowledgement is design to solve the three of six weaknesses of watchdog scheme namely

1) Receiver collision

2) Limited transmission power

3) False misbehaviour.

1. Receiver collision: - As shown in the figure 3 once node A sends Packet1 to node B, it tries to take in if node B forwarded this packet to node C; in the meantime, node X is forwarding Packet2 to node C. In such case, node A overhears that node B has with success forwarded Packet 1 to node C however did not observe that node C is failed to receive this packet as a result of a collision between Packet 1 and Packet2 at node C.

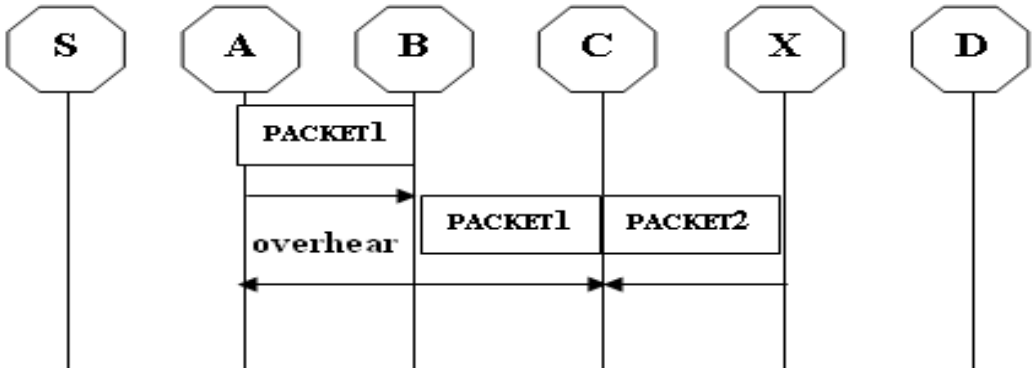

Fig.3 Receiver Collisions

2. *Limited transmission power:-* As shown in the figure 4 of limited transmission power to manage battery resources node B limits its transmission power so that it is very strong to overheard by node A after transmitting power but it's too weak to reach at node C because transmission power is reduced at certain limit.

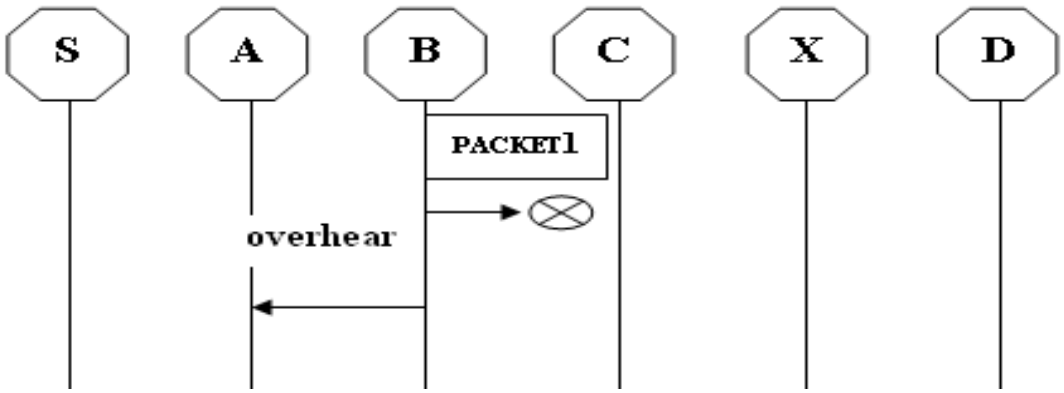

Fig.4 Limited Transmission Powers

***3. False misbehave* :-** As shown in the figure 4 even though node A and node B send packet1 successfully to node C node A still inform node B as misbehaving due to open medium and remote distribution of typical manets. Attackers can add one or two nodes to achieve this false misbehavior report attack. Two ack and AACK can solve this problem of limited

power transmission as well as receiver collision but both are fail to solve the problem of false misbehavior attack. In order to solve receiver collision, limited transmission power as well as false misbehavior attack the EAACK (enhanced adaptive acknowledgement) is introduced [1].

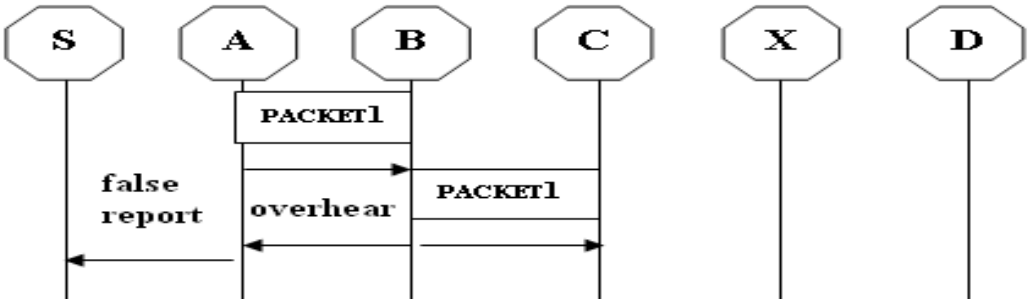

Fig.5 False Misbehave

IV. PROPOSED SYSTEM

EAACK is consisting of three major part as acknowledgement (ACK), secure acknowledgement (S-ACK) and misbehaviour report authentication (MRA).

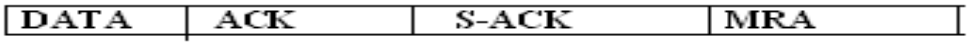

Fig.6 EAACK Protocol in Manets

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 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 [4]. 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: - This field is designed to solve the problem of watch dog when it is fail to detect misbehaving nodes with the presence of false misbehavior. False misbehavior report may be able to generate by malicious attackers to falsely report innocent nodes as malicious. 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 route 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.

A. Digital signature:

EAACK is acknowledgement base intrusion detection system. All the three fields of EAACK i.e. (ACK, S-ACK and MRA) all are acknowledgment based they rely on ack to detect misbehave nodes in the network. Hence it is very essential to verify that all acknowledgment packets in EAACK are authentic and untainted. For this digital signature is necessary. 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]. So hence for all the acknowledgements should be digitally signed and for that DSA algorithm is used.

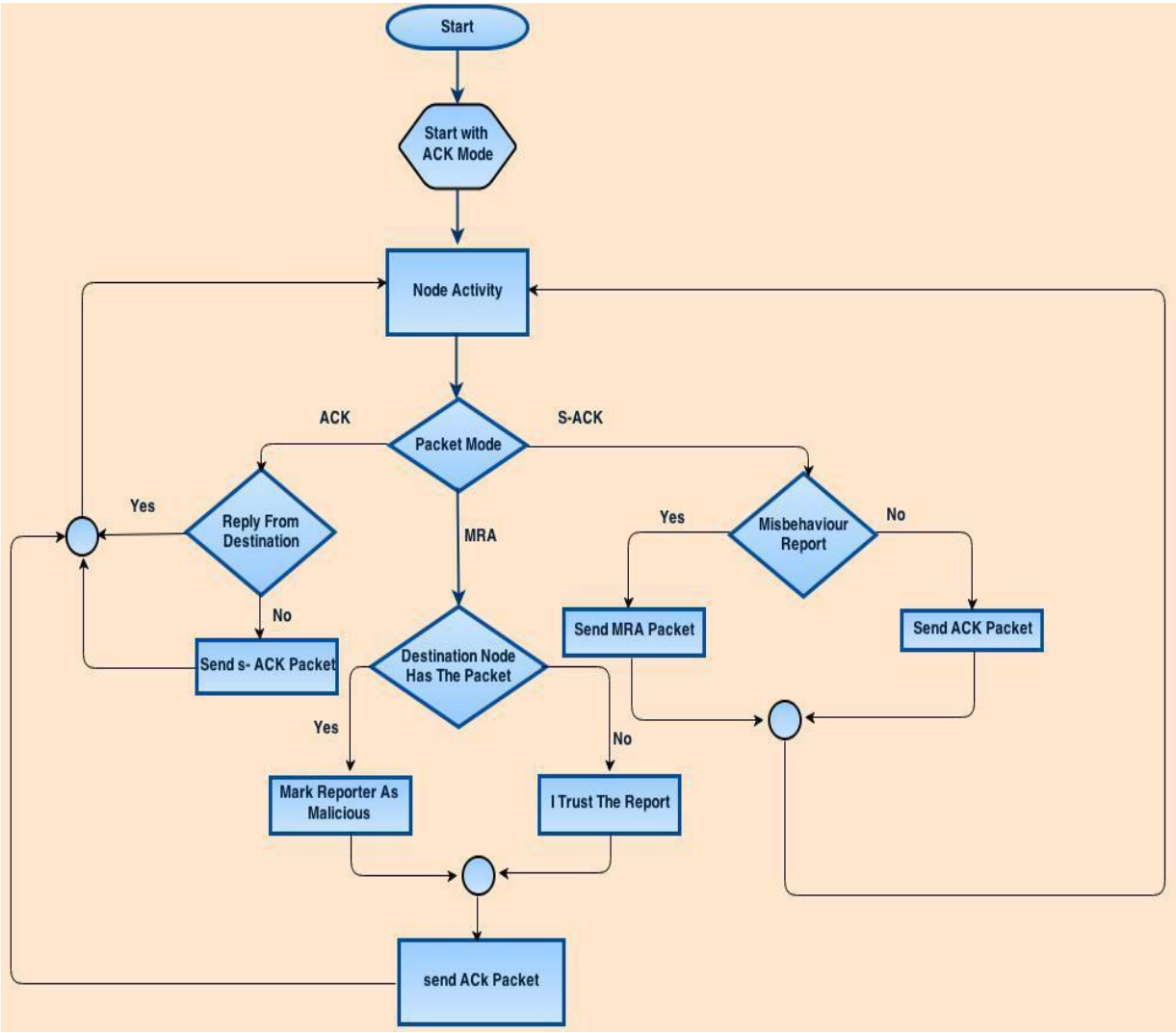

Fig.7 System Flow Of EAACK

V. COMPARISM BETWEEN THE EXISTING SYSTEM AND PROPOSED SYSTEM

TABLE I. COMPARISM BETWEEN THE EXISTING SYSTEM AND PROPOSED SYSTEM

Parameters	**Existing system**	**Proposed system**
Overhead bits	More	less
Security	less	more
Limited transmission power problem	Not solved	solved
Malicious nodes	Not detected	detected
Receiver collision	occurs	Not occurs
False misbehave problem	Not solved	solved
Attacks	possible	Not possible
Partial dropping error	Not solved	Not solved
Ambiguous collisions error	Not solved	Not solved
Mechanism for security	Not used	DSA or RSA algorithms are used

VI. CONCLUSION

In this paper EAACK intrusion detection system is detect the misbehave report in the network. This was not possible in watchdog as well as in the TWO ACK schemes. So many drawbacks of existing systems are overcome in this system. This system is used for discovering malicious nodes and attacks on Manets. The EAACK system is very much secured than the existing system. The proposed system is solving the three of six weaknesses found in existing system. In future it will compare with popular mechanisms. Security is main issue in Manet so partially it is satisfied by EAACK intrusion detection system. So in future try to overcome all the drawbacks of watchdog. Security can be tackle by cryptography. In future try to solve the remaining problems of existing system.

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 Publishers.

[4] 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.

[5] Kejun Liu and VarshneyMay, "An acknowledgment-based approach for the Detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, May 2007.

[6] Nidal Nasser and Chen Y, "Enhanced Intrusion Detection Systems for discovering malicious nodes in mobile Adhoc network," in Proc.IEEE Int.Conf. Commun. Glasgow, Scotland, Jun 2007.

[7] Rajaram and Gopinath, "Efficient Misbehavior Detection System for MANET," Dec 2010.

[8] Rajyalakshmi and Anusha, "Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System, "July 2013.

[9] Rivest and Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun.ACM, vol. 21, no.2, pp. 120–126, Feb 1983.

[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.