ISSN:2249-5789
SURAJ MAHAJAN ET AL , INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & COMMUNICATION NETWORKS,VOL 5(2),154-159

Enhanced , ntrusion ' etection Algorithm in MANET

[1]Suraj mahajan, [2]amit Welekar
[1,2]Department of Wireless Communication and Computing, RTMNU University, TGPCET ,
Nagpur, Maharashtra, India
{suraj.mahajan123@gmail.com, welekar.amit@gmail.com}

Abstract: - In Present years, in mobile ad hoc network security is more concerns. As comparison to wired network the MANET is more exposed to attack. Because of its Properties, such as, limited power and limited bandwidth, it is very difficult to get security in ad hoc network topology. The techniques we use today like encryption and authentication are not enough for minimizing the possibilities of attacks. However, those techniques are to prevent for a limited set of possible known attacks. Those techniques are not able to prevent newer attacks that are made in the existing security measures. For this enhance mechanism is required to prevent or detect never attacks. The objective of this paper is to classify current techniques of enhanced Intrusion Detection System (IDS) aware MANET. In this paper we have study various intrusion detection techniques in MANET and then the comparison among several researches achievement will be evaluated based on their parameters and detection technique.

Keywords: Mobile Ad hoc network, Security, Intrusion detection, Survey.

I. INTRODUCTION

Due to the mobility and easy to use wireless network is preferred from the day of their invention .because of the new adaption of advance techniques and reduce cost wireless network preferred more than wired network. Ad hoc network is a collection of small infrastructure mobile nodes with both transmitter and receiver that communicate with each other within a prescribed limit of coverage .controlling via a wireless network is becoming very popular now a day. Due to wireless network it is possible to allow communicate with maintain their mobility. This communication is limited for the range of transmission. If two nodes cannot communicate with each other than MANET allowing intermediate note to solve this problem.

MANET dividing their network into two types namely, single hop and multi hop. For single hop network communication within a range is directly. On other hand in multi hope network if transmission is out of radio range then it rely on other intermediate node for transmission. In contrary to the traditional wireless network, MANET has decentralized network infrastructure. It does not require a fixed infrastructure.

This unique characteristic makes MANET more special in industrial area and network security. The open medium and remote distribution of MANET make it vulnerable to various attacks. Because of lack of protection and security attackers can easily capture. MANET consist of distributed architecture and having changing topology it is not possible for centralize technique to monitor properly for MANET .It is required to develop an intrusion detection system which is required for MANET. For enhancing the level of security intrusion detection system should be added. If MANET is able to detect the attack before it enters the system it will protect the system from damage and it act like a layer in MANET.

Mobile Ad hoc NET works (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either indirectly or directly. One of the major advantages of wireless networks is its ability to allow data communication between many parties and still maintain their mobility. However, the range of transmitters is limited for this communication. This means that when the distance between the two nodes is beyond the communication range of their own these two nodes cannot communicate with each other .

MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET mainly into two types of networks, namely as, single-hop and multi-hop network. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In compare other networks to the traditional wireless network, MANET has a decentralized network infrastructure.

Owing to these unique characteristics, of MANET is becoming more and more widely implemented in the industrial area. However, thus considering the fact that MANET is popular among critical mission applications, network security has a vital importance. Unfortunately, the open medium and the remote distribution of MANET make it more vulnerable to various types of attacks. For example, due to the malicious attackers can easily capture, nodes' lack of physical protection and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs by inserting malicious or non-cooperative nodes into the network assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise by MANETs .

Furthermore, because of MANET's changing topology and distributed architecture, a traditional centralized monitoring technique is no longer feasible in MANETs. In such a case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs by using Advance encryption technique with the help of new hybrid cryptography to reduced overhead of network for existing system.

II. Literature survey

The ability of self-configuring made it popular among military application or emergency recovery. Wide distribution makes MANET vulnerable to attackers. In this they propose new intrusion detection named enhanced adaptive acknowledgement design for MANET. It is crucial to develop efficient mechanism to protect MANET from malicious attaches .EECK demonstrate higher and enhance malicious behavior detection mechanism for MANET [1].

1.1 HISTORY OF IDS:

An intrusion-detection system (IDS) can be described as resource and method to identify, assess, and report unauthorized or unaware or malicious network activity. Intrusion detection is typically part of a protection system that is installed around a system and act like a second layer for MANET it is not a stand-alone protection system measurement.
Based on their detection techniques intrusion detection system classified into three main categories as follows

- Signature or misuse based IDS)
- Anomaly based IDS
- Specification based IDS,

It is a hybrid both of the signature and the anomaly based IDS. Also known as signature based detection mechanism, a standard rule or a regular sequence of actions or events are used to match an attack. There are many methods in the signature detection, which they differ in matching algorithm employed to find the intrusion patterns and presentation. In anomaly comparison in between normal and capture user system takes place. Result of those comparison IDS will detect the anomaly. detection has several techniques statistics, neural networks and other techniques such as data mining In Specification based detection, some define constraints are taken and it monitor regularly if any mismatch will happened then it take it as a or reported as attack, like watchdog technique.

Ad hoc Network, it is a collection of mobile nodes without having any proper base infrastructure. MANET is a network which contains collection of nodes containing their transmitter and receiver which communicate with bi-directional links directly or indirectly. A new enhanced intrusion detection system named Enhanced Adaptive Acknowledgement designed for MANETs. By the adoption of MRA scheme. Enhanced system is able to capture the malicious nodes and

report it as a malicious node and it compare with other technics. The result of this demonstrates the positive performance against two acknowledgement system and watchdog techniques. This technique is the case off limited power consumption by the nods and misbehavior of malicious node and it limiting the power off transmission because of acknowledgment by the receiver.

The use of mobile ad hoc network increases as the technology enhancing in many application. Due to the distributed architecture off MANET it vulnerable to attacks.. Because of increasing the use of wireless system it required to be a completely secure transmission Due to some special characteristics of network it require to a system more secure hence by using many intrusion detection technique we detect the malicious node .There have some different characteristics of AD HOC network we discus in this pepper.. Due to open medium of MANET and no centralise monitoring it is more venerable to the attacks. Due to such distributed topology it is not able to detect or remove such vulnerable attack by encryption and authentication. Anomaly is powerful tool to detect attacks because existing system is only removing the attack. This paper we have the characteristics of MANET, attacks and comparison of existing IDSs.

In this paper we discuss the routing misbehavior in mobile ad hoc network, routing protocol based on all nodes in network are co-operative and authorized for communication. Because of open structure and distributed topology node misbehavior exists. In routing misbehavior nodes take part in discovery of route and process of maintenance. In this paper, propose the two acknowledgement scheme for misbehavior in routing and their effects.

MANET does not require a fixed infrastructure. All depends on distributed technology. Nodes within a range will communicate directly through node to node. Every node transmits and receives through same node. Self-configuring ability of node makes it popular among some specific application but open medium of nodes makes it more vulnerable to attacks by malicious node. It is required an advance mechanism for finding intrudes by intrusion detection technique. Nature of new feature need to enhance a live setting,. Enhance technique is more reliable to detect and remove the attacks. There are many techniques implemented but all have problem for acknowledgment enhance technique gives the information about packets report and their details. Their IDS named EAACK for detecting the forged acknowledgment.

The Major challenge in mobile ad hoc network is their dynamic nature and no centralize monitoring and distributed infrastructure, which require more secure and attack free environment to travel data more securely. In this dynamic nature of MANET is more challenging for security point .this paper compares three routing protocols DSDV, DSR and AODV, with consideration of their node concern .we discuss before paper node misbehavior can detect through IDS, and This paper discuss co-operative Intrusion Detection, watchdog technique and path ratter .which are more effective than other techniques.

In dynamic routing conventional protocols is not possible because they have distributed nodes .For example, in dynamic environment like ad hoc network topology must be changed when packet data is routed. The quality required is must be variable in distributed topology. In terms of wired network structure is static. MANET is basically classified as reactive routing proactive routing and hybrid routing. Total network throughput can be increase by using all nodes for forwarding. Due to increasing nodes for packet routing bandwidth required is less.

Routing Protocols:
Basic categories of routing protocol are proactive routing protocol and reactive protocol. Proactive routing is also called as table driven protocol. it rely on table which contain all possible information regarding the routes about possible destinations, where as in reactive routing it depends on demand source initiated route. In this technique route is created depends on requirement. This paper is compare table driven protocol with most popular on demand routing protocol. Proactive routing is work on a table driven mechanism, all mobile nodes contain routes for all destination with multiple hopes in between. Each entry in the route is marked as per their sequence by the destination node. With the use of sequence malicious node can determine and routing loop can be determined.

As discussed before EAACK is based on acknowledgement, all are rely on acknowledgment packet to detect misbehaviour in the network. It is required to ensure all packets that are acknowledged are authentic. The scheme is vulnerable to malicious attack If attackers are smart enough to read the packet data. Hence it is required a digital signature to remove above difficulties. In this scheme required all packet with digitally signed before transmit. Digitally signed packets are sent and it is verified first before they accept at the destination. There for resource required for digital signature in MANET is more.in this paper they implement both DSA and RSA, behind this is to get most optimal solution for digital signature in MANET. It is a part of cryptography. Cryptography is the mathematical based module of security such as authentication; data integrity etc. Digital signature is widely used technique to ensure authentication and data integrity of MANET. Digital signature is mainly classified as
Signature with appendix: In this message is required in verification algorithm. Like DSA.

Message recovery: This technique only required a signature inverification process. Like RSA. We are considering the Routing misbehavior in MANETs (Mobile Ad Hoc Networks). Routing protocols for MANETs are based on the assumption which have, all the participating nodes are fully cooperative. But, due to the open structure node misbehavior's may exist in the network. One of such routing misbehavior is that some nodes will take part in the route discovery and maintenance processes but refuse to forward data packets. In this, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their effect.
Limitations: No security over the data.

The dynamic nature is the major challenge to design and deployment of mobile ad hoc networks (MANETs), which consist of a set of security measures to be resolved. In this work, we compare the behavior of three routing protocols DSDV, AODV and DSR, with the consideration of the node misbehavior. This problem of misbehavior of nodes can be detected and controlled by different techniques such as Intrusion Detection System (IDS), watchdog, Cooperative Intrusion Detection and path rater discussed in this paper which is more efficient than other general techniques.
Limitations: They focus on routing the data.

Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. By the adoption of new MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report and compared it against other most popular mechanisms in different scenarios through simulation. These results will demonstrate positive performances against TWOACK, Watchdog and AACK in the cases of false misbehavior report, receiver collision and limited transmission power. EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.
Limitations: Not sufficient to adopt to changing security threats.

The self-configuring ability of nodes in MANET made it popular among emergency recovery or critical mission applications like military use. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this way, it is very crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the cut in hardware costs and improvements in the technology, we are witnessing a current trend of expanding MANETs into industrial applications. We strongly believe that it is vital to address its potential security issues to adjust to such a trend. In this work, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. While does not greatly affect the network performances compared to contemporary approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances.
Limitations: Due to use of DSA overhead of network is increased.

III. Proposed Work:

1. Adaptive similarity:
Design a system having number of nodes without central monitoring .The technique used to detect a malicious nodes and remove it before it affect the data and enter into the system node. It works without any fixed infrastructure

network. It is having open and wide distribution network topology.

2. Keyword expansion:
In enhance technique we use digital signature technique with enhancing the acknowledgment technique of two acknowledgments and remove the drawback of acknowledgment problem. By enhancing the algorithm malicious nod can detect before it affect the nodes. Overcome the problem of vulnerable attackers.

Problem Formulation:

1. Enhancing intrusion detection technique for MANET.
2. For data to the destination is reach is not guaranteed because of malicious node.
3. To detect malicious node and remove it from network.
4. Provide strong authentication And Acknowledgment system.

Objectives

The primary objectives of this study can be summarized as follows:

1. For authentication we will use advanced encryption technique.
2. Develop enhanced intrusion detection system.

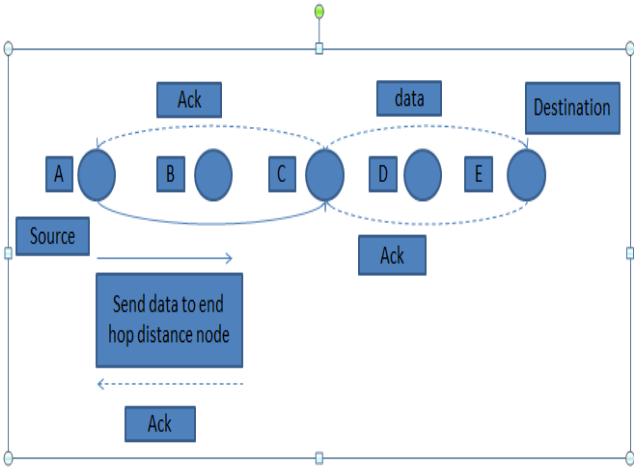
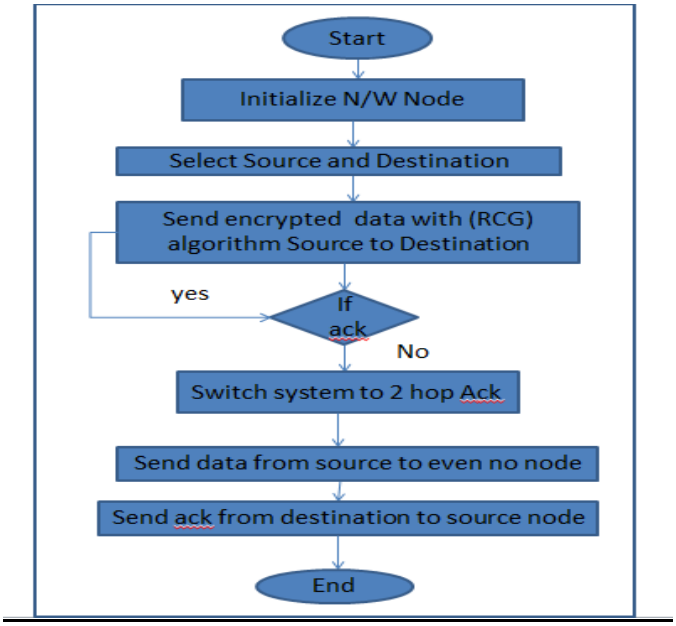


Figure No

1. Data Send A to C
2. Ack from C to A
3. Data Send C to E
4. Ack from E to C &then C to A.

Research Methodology/Flow chart:



Flow chat of proposed algorithm

Uses of new algorithm RC6. This technique we distribute/divide 128 byte data into 4 parts in which 32 byte each. System improves the security level of system. Each A, B, C & D all of 32 bytes each is equal to 4! Data encrypt in 4! Times like ABCD, ABDC, ACDB, ADCB, BDCA etc.

IV. Result &Comparison of Graphs:

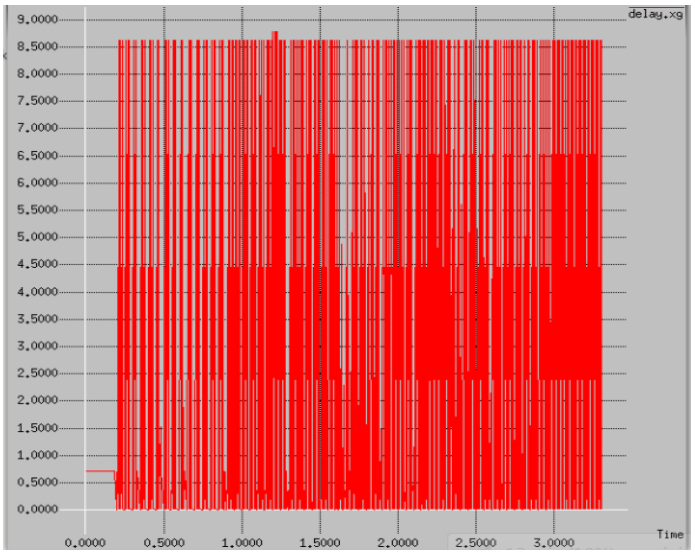


Figure No Existing System with one hope

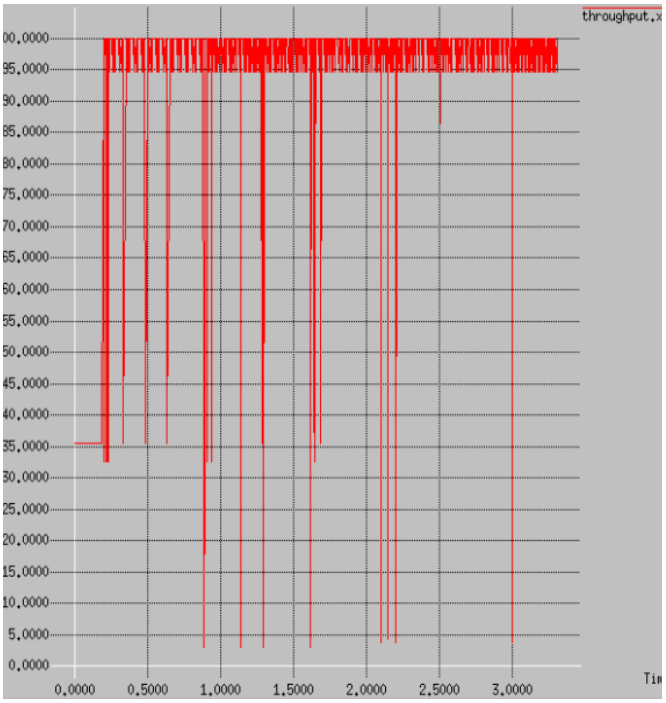


Figure No : Throughput Graph of existing technique

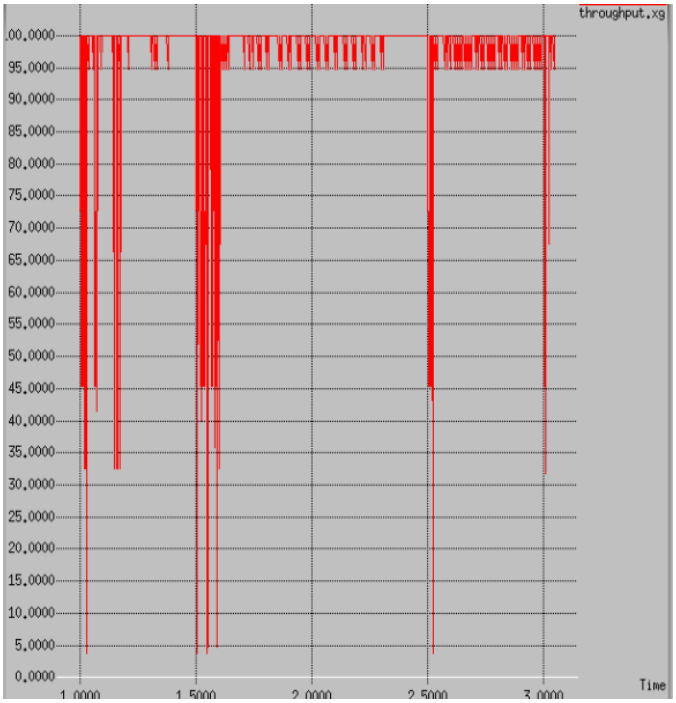


Figure No: Throughput Graph of two hope

Throughput Graph = Output/ Input

Graph of efficiency i.e. packet dropping happened or not

Delay Graph: It is the time delay from source to destination

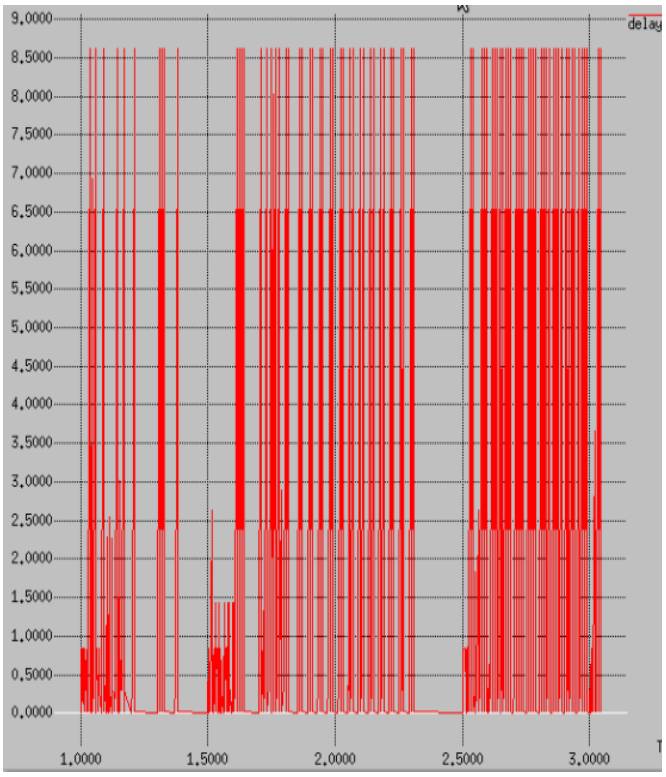


Figure No: System with two hopes

V. CONCULSION

In MANET security over data and packet dropping is major issue. In this paper digital signature and enhance algorithm is adapted for detect attacker. It compare against exiting system in MANET. Enhance technique is monitoring on routing the data. To improve the existing system and packet dropping new hybrid technique is adapted.

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] Y. Kim, “Remote sensing and control of an irrigation system using adistributed wireless sensor network,” IEEE Trans. Instrum.Meas., vol. 57,no. 7, pp. 1379–1387, Jul. 2008.

[3] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting misbehaving nodes in MANETs,” in Proc. 12th Int.

Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[4] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[5] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[6] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

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

[8] 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.

[9] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[10] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[11] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf.Perform., Comput.,Commun., 2004, pp. 747–752.

[12] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78Analysis of the Information Value of User Connections for Video Recommendations in a Social Network.

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

[14] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, "Energy harvesting from piezoelectric materials fully integratedin footwear," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819,Mar. 2010.

[15] T. 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.

[16] 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.

[17] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[18] 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.