A New Enhanced Adaptive Acknowledgment Secure Intrusion Detection System for Mobile Adhoc Networks

Panga Narasimha Murthy [#1]**, M M M Kumara Varma** [*2]

M.Tech Scholar [#1], Associate Professor [*2]

Department of Computer Science & Engineering,
Sri Sivani College of Engineering, Chilkapalem,
Etcherla Mandal, Srikakulam District.532402.

Abstract

In recent days there was a lot of demand for wireless sensor networks compared with wired networks as lot of users have been migrating to wireless sensor networks from wired network .This is mainly due to the mobility and scalability functions which was brought by WSN.As this was increasing its attention of spreading almost all around the world, there was a lot of intruders who try to attack the data transmission during WSN communication. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. For identifying the suspicious objects or intruders in wireless sensor networks there was no proper system until an Intrusion Detection System (IDS) has been proposed. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for

MANETs. Compared to contemporary approaches, EAACK demonstrates higher –behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Keywords

WSN, IDS, MANETs, *Terms*—Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK),

1. Introduction

A Wireless Sensor Network (WSN) is a collection of several nodes ranges from a few to several hundreds and even thousands of nodes, where each and every group of nodes is connected either to single sensor or group of sensors. Sensor network typically has several parts which is clearly shown in figure 1.

1. A radio transceiver device with an inbuilt internal antenna or device connected to an external antenna.

2. A microcontroller

3. An electronic circuit board for interfacing mainly with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

Sensor may be vary in size when compared with different type of sensors just like of a shoebox down to the size of a grain of dust. The amount for purchasing of single sensor nodes is similarly variable in its price, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. While deploying any sensor some valuable resources like energy, memory, computational speed and communication bandwidth mainly depends on size and cost of the sensor what we use. The topology (I.e. arrangement of nodes) of the WSNs can vary from a basic star network to an advanced mesh network. The propagation technique between the nodes of the wireless network can be routing or flooding [1], [2].

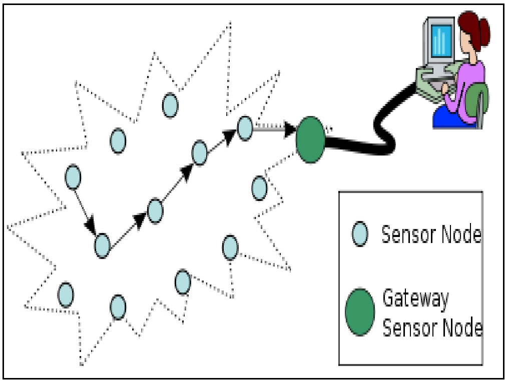


Fig.1. Represents the typical multi-hop wireless sensor network architecture

Recently with the huge usage of wireless sensor networks in a variety of applications, a lot of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs.For the general purpose network deployment, normal WSN cannot able to fulfill the needs like sensing range, transmission range, and bandwidth range for sensing the data remotely. To achieve this, it is very crucial to identify the impact parameters of network on its performance w.r.t application specifications. In CSE and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year for the improvement of its performance**[**3],[4].

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [14]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. Many research efforts have been devoted to such research topic [6]–[9], [15], [16]

2. Background Work

In this section, we will find the information which was very near to our current intruder detection system in detail.

Intrusion Detection System

An **Intrusion detection system** (**IDS**) is internet software which is mainly deployed on the hardware designed to detect any unwanted attempts to access, manipulating, and/or disabling of computer mainly through a network. An intrusion detection system is mainly used to identify several types of malicious behaviors that can easily compromise the security and trust of a computer system. Some of the attacks include network attacks against vulnerable services, host based attacks such as privilege escalation attack, unauthorized logins attack and attempting to access some invalid files like viruses and worms.

IDS are mainly composed of several components:

1. Sensors: This is used for generating security events.

2. Console: Which is used to monitor events and alerts, while controlling the sensors.

3. Central Engine

Which is mainly used for recording the events logged by the sensors in a database and use a system of rules to generate alerts from security events received.

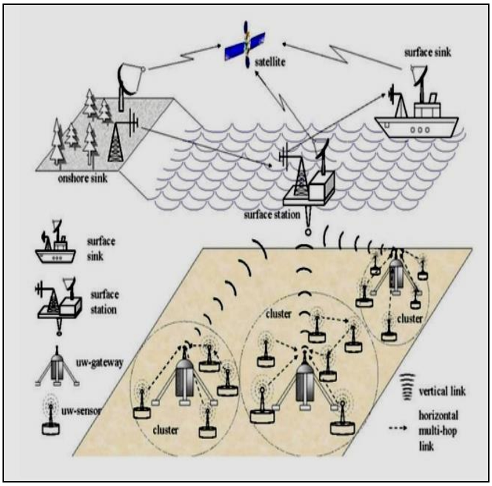


Fig.2. Represents the Military application which uses wireless sensor network

Intrusion detection system software is basically executed and deployed in wireless sensor networks. The development of such a variety of wireless sensor networks was originally motivated by military applications such as battlefield surveillance and attacker identification through sensor which is clearly shown in figure 2. However, now a days these wireless sensor networks is also used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

3. Existing Approaches of MANET's

In this section, we mainly describe three existing approaches, namely, Watchdog [17], TWOACK [15], and Adaptive ACKnowledgment (AACK) [18].

1) Watchdog:

Marti *et al.* [17] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node 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, 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.

2) TWOACK:

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [16] is one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming 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) [11]. The working process of TWOACK is shown in Fig. 3:

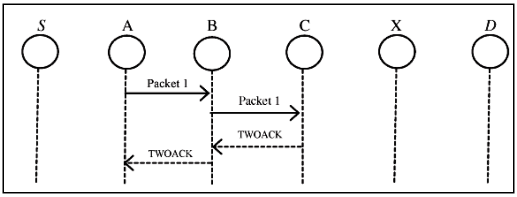


Fig. 3. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which 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 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

3) AACK:

Based on TWOACK, Sheltami *et al.* proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK).

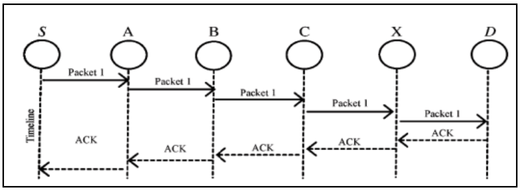


Fig. 4. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 4.

4. Proposed EAACK Scheme

In this section, we describe our proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work [12], where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets.EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [11], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I.

Fig. 5 (shown later) presents a flowchart describing the EAACK scheme. Please note that, in our proposed scheme, we assume 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. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

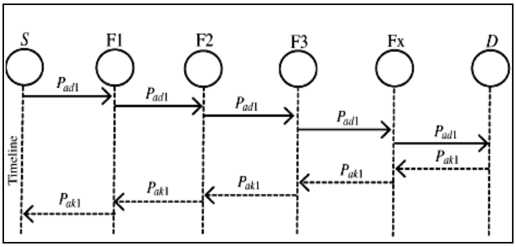


Fig. 5. System control flow: This figure shows the system flow of how the EAACK scheme works.

4.1 ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 6, in ACK mode, node S first sends out an ACK data packet *Pad*1 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 *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, 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.

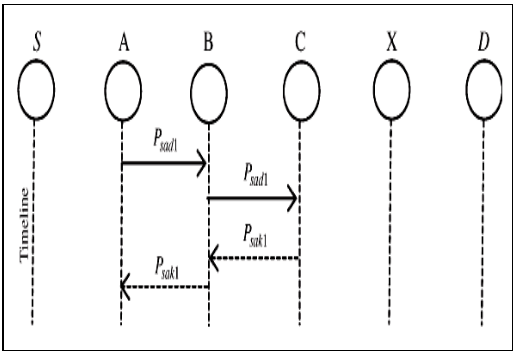


Fig. 6. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

4.2 S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [16]. 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. As shown in Fig. 7, in S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet *Psad*1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives *Psad*1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node F2. Node F2 forwards *Psak*1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

4.3 MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme 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

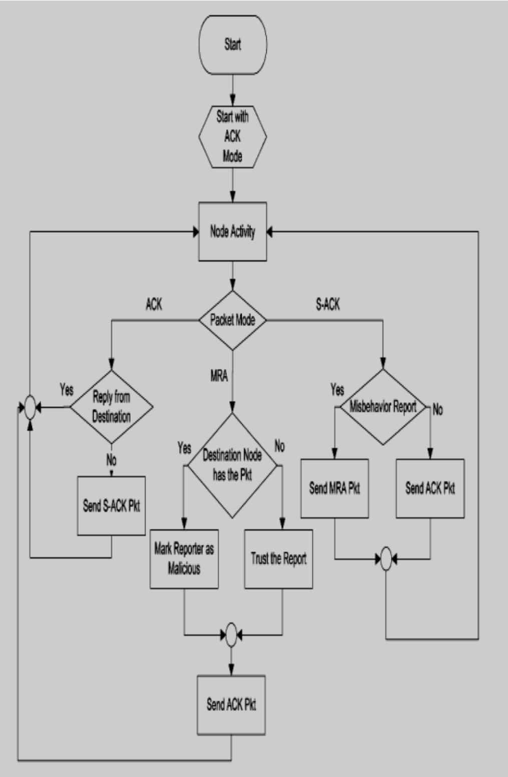


Fig.7. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

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.

By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

4.4 Digital Signature

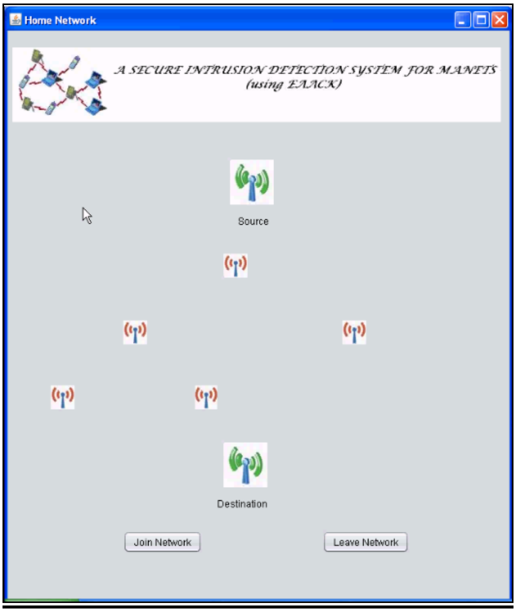
As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

5. Experimental Results

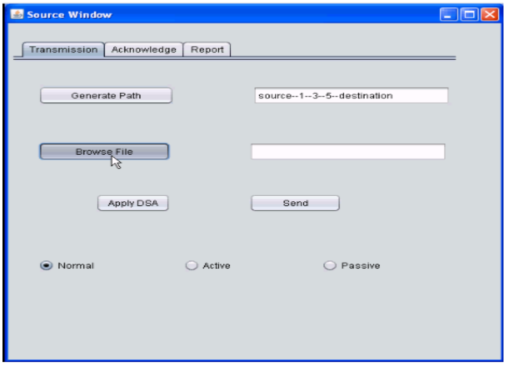
We have implemented the proposed concept on Java Platform in order to show the performance of our proposed EAACK scheme is very accurate in identification of attacker when compared with various existing models.

5.1 Main Window

The below window clearly shows that this is the main window for entering into the application, this was designed with Java Swings as a front End user interface.



5.2 Source Window



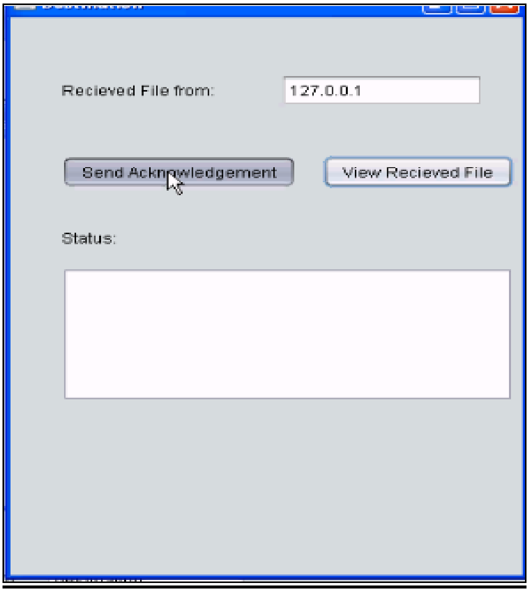
source--1--3--5--destination

● Normal ○ Active ○ Passive

The above window clearly justifies that this is a Source window through which the user can communicate with the destination window.

5.3 Destination Window

The below window clearly represents that this is the destination window which is used for interacting with the source window.



Recieved File from: 127.0.0.1

6. Conclusion and Future Scope

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network’s PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

Future Enhancement

To increase the merits of our research work, we plan to investigate the following issues in our future research:

1. Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.

2. Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre distributed keys.

3. Testing the performance of EAACK in real network environment instead of software simulation.

7. References

[1] Dargie, W. and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010 ISBN 978-0-470-99765-9, pp. 168–183, 191–192.

[2] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications, John Wiley and Sons", 2007 ISBN 978-0-471-74300-2, pp. 203–209.

[3]http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6550437.

[4]http://www.thinkmind.org/index.php?view=article&articleid=icn_2014_3_40_30195

[5] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered
wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*,
Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582,2007.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

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

8. About the Authors

Panga Narasimha Murthy is currently pursuing his 2 Years M.Tech (CSE) in Computer Science and Engineering at Sri Sivani College of Engineering, Chilkapalem, Etcherla Mandal, Srikakulam District. His area of interests includes Networks security and Information Security.

M M M Kumara Varma is currently working as Associate Professor, Dept. of CSE at Sri Sivani College of Engineering, Chilkapalem, Etcherla Mandal, Srikakulam District. His research interests include Networks, Information Security, Data Mining.