ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

GeRaF with EAACK- A Secure and Efficient Intrusion Detection System for MANET

Agna Jose E

Department of Computer Science, Royal College of Engineering & Technology, Akkikkavu, University of Calicut, Kerala, India

ABSTRACT: Now a day we used many applications based on the mobility and scalability. Among all the wireless networks, Mobile Ad hoc Network (MANET) is one of the most important and popular network. MANET consists of mobile nodes which can move freely. MANETs are highly vulnerable for passive and active attacks because of their open medium, rapidly changing topology, lack of centralized infrastructure. It is crucial to develop suitable intrusion detection scheme to protect MANET from malicious attackers. In base paper they proposed a mechanism called Enhanced Adaptive ACKnowledgement (EAACK) scheme. Nevertheless, it suffers high routing overhead. So I introduce Geographic Random Forwarding (GeRaF) into the EAACK scheme, and investigate the performance of this system in MANET. This will give high security for packet transmission and high efficiency in routing.

KEYWORDS: EAACK-Enhanced Adaptive Acknowledgement, GeRaF-Geographical Random Forwarding, IDS-Intrusion Detection System.

I. INTRODUCTION

Wireless network is a computer network in which all communication modes are wireless. A very attractive category of wireless network is based on Adhoc topology. Ad-Hoc mainly means that there is wired infrastructure for communication. Figure 1 [2] shows Ad-Hoc and infrastructure topologies.

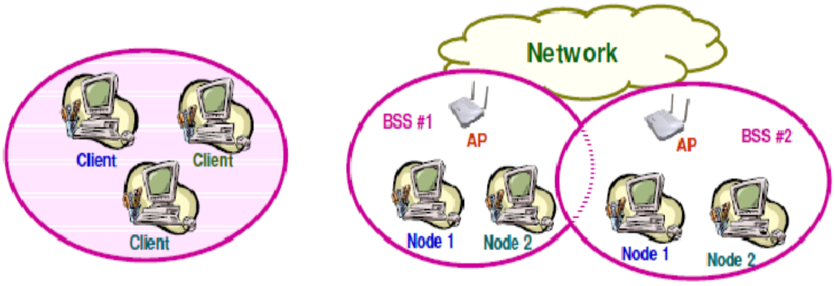

Fig 1 Ad-Hoc Networks

Wireless Adhoc network can be classified in to three categories.

- Mobile Ad-Hoc network (MANET)
- Wireless Sensor network
- Wireless Mesh network

Each of these is significant in different situations and differs in the capacity and capability of nodes that participate in the network. This paper is focusing on MANET. A typical MANET is shown in figure 1 [2]. The circles in the figure indicate communication ranges of individual nodes.

DOI: 10.15680/ijircce.2015.0305165

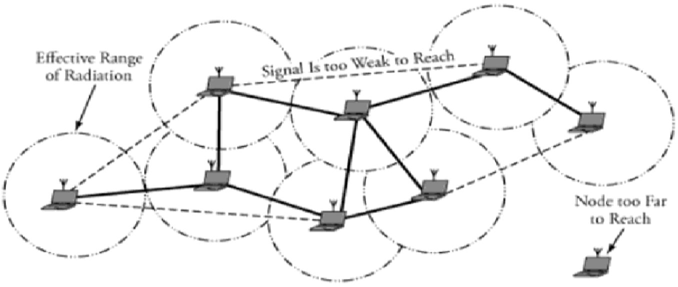

Fig 2 MANET

The two main significant differences between infrastructure based and Ad-Hoc networks are:

- Communication in Ad-Hoc network are truly peer to peer
- Individual nodes that do processing itself are required to route packets.

These may make some challenges in Ad-Hoc network

CHALLENGES IN MANET

MANET suffers from limited computational measures, low battery power and changing topologies. So building routing decisions is a very big challenge. The most important challenge is of security. The main goal of security measurements in MANET is to protect the information and resources from attacks and misbehavior. A secure protocol which satisfies the following requirements will help to win this challenge.

- Availability: Availability of the required network services when desired.
- Confidentiality: Securing the information from unauthorized access.
- Authenticity: Ensuring communication from mode to other as genuine.
- Integrity: Ensures that a message was not modified by a malicious mode during transmission.
- Non – repudiation: Ensures that the origin of the message is legitimate.

WIRELESS NETWORK ATTACKS

Ad-Hoc Network modes are low battery powered devices and placed inside the mobile units. This help the attackers to access the network very easily. Hence many users of the Ad-Hoc network are in public places and revealing secrets unintentionally, attackers can overhear the communication with little effort. Some of such attacks are shown in the following fig 3.

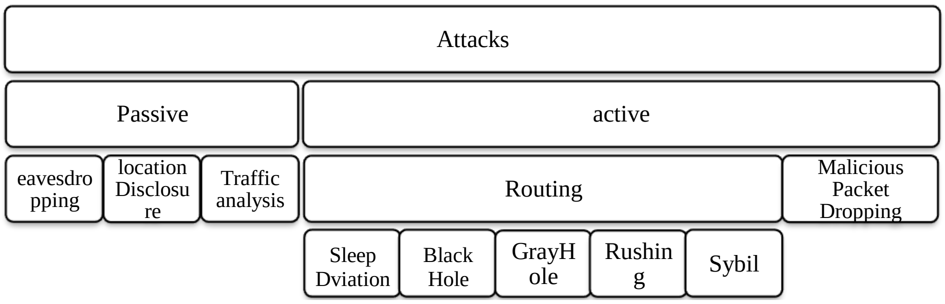

Fig 3 Different types of attacks

INTRUSION DETECTION SYSTEM

The medium of MANET is wide open. There is no distinction between usual and unusual activities. So malicious users as well as legitimate users can access the network and can produce false routing information.

Encryption and authentication can be used as an intrusion prevention technique. But it is considered as a thin layer of defense and is not sufficient for MANET. As the network become more dense, weakness also increases and leads to more security issues. Hence intrusion detection systems are developed as a second wall of defense. A response can be initiated when an intrusion is detected, which will prevent or minimize the damage to the system.

IDS consider a number of assumptions to work. First assumption is that all the activities can be observed. And the assumption is that the normal and intrusive activities have different behaviors, which can be captured and analyzed by the IDS when the network has another node.

II. RELATED WORKS

We have many researchers have done research in the area of IDS in MANET. Most of them are related to routing protocols. But still they couldn’t find Intrusion Detection System with both security and efficiency.

Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker describe two techniques [1] called watchdog and pathrater that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To solve this problem, propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a path-rater that helps routing protocols avoid these nodes. watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of ambiguous collisions, false misbehavior, collusion, receiver collisions, limited transmission power, and partial dropping.

Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker overcome the weakness of Watchdog and introduce an intrusion detection system [2] called ExWatchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Compared to Watchdog, solution has the same advantages. At the same time, it solves one big weakness: false misbehavior. False reporting may result in network partition and further decrease network performance. However, there is limitation in our solution. If the real malicious node is on all paths from specific source and destination, then it is impossible for the source node to confirm with the destination of the correctness of the report. For this case, we do not and cannot take any action because we do not know who lies and cannot either check.

Kejun Liu, Jing Deng Pramod K. Varshney and Kashyap Balakrishnan propose [3] the 2ACK scheme to mitigate the adverse effects of misbehaving nodes. The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. Such a 2ACK transmission takes place for only a fraction of data packets, but not all. Such a “selective” acknowledgment1 is intended to reduce the additional routing overhead caused by the 2ACK scheme. Judgment on node behaviour is made after observing its behaviour for a certain period of time.

Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami proposed [4] EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). 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. 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. The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. [3]. 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. 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 this scheme. The MRA scheme is designed to resolve the weakness of Watchdog [1] 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

DOI: 10.15680/ijircce.2015.0305165

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 and seeks for an alternative route to the destination node.

Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami describe Enhanced Adaptive ACKnowledgement version 2 [5] (EAACK2) scheme. This scheme is based on our previous research EAACK [4]. Compared to EAACK, EAACK2 provide 2 additional features. First is Acknowledgement authentication. It will Prevents attackers from forging fake acknowledgement packet and thus conceive its malicious misbehavior. Second feature is Packets integrity. This will Prevents attackers from contaminate packets in MANETs. But Both EAACK And EAACK2 has very high routing overhead. So I would like to implement a new method called Geographical random Forwarding (GeRaF) in EAACK. This will reduce routing overhead and will provide performance almost equal to ideal packet transmission.

III. SYSTEM MODEL

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). 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.

ACK Scheme

Normal packet transmission done by this scheme. If we send a packet Pad1 from source S to destination D through A, B, C. After receiving the packet in destination it must resent a acknowledgement packet Pack1 to source.

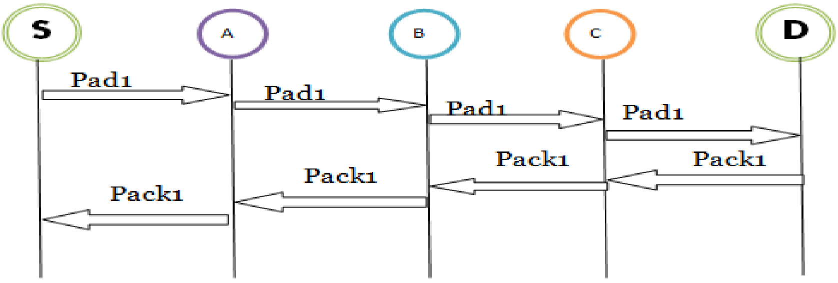

Fig 3 ack scheme

If the acknowledgement packet received securely within a predefined time period send next packet. If the acknowledgement packet is not received securely within a predefined time period shifted the packet mode to S-ACK.

S-ACK Scheme

S-ACK scheme detect by acknowledging every data packet transmitted over every three consecutive nodes along the path from source to destination. Every node along the path need to send back a secure ack packet to the current node to the node which is 2hop away from it back.

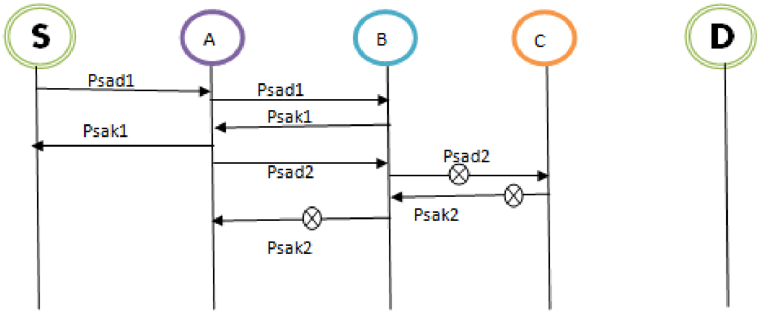

Fig 4 S-ACK scheme

If node A doesn’t receive s-ack packet with in a predefined time period, both B and C are reported as malicious. Then misbehaviour report is generated by A is send to Source. By this source will switch to MRA mode.

MRA (misbehavior report authentication)

This scheme authenticate whether the destination node has received the reported missing packet through another route. For that, we first search for an alternative route to destination. Then sent a MRA packet from S to D through that alternative path. After receiving in the destination, it searches its local knowledgebase and compares if the reported packet was received. If it was already received, then it concludes that this report is false report and marks the node whoever generates this report as malicious. Then avoid the malicious node in future transmission.

In MANET we can find multiple paths between pair of nodes. By choosing an alternative route source can circumvent the misbehavior reporter node. When the node D receives an MRA packet, it looks in to its local knowledge base and check if the reported packet was received. If it is received, then conclude that this report is a false misbehavior report and reporter, whoever generated this report is marked as malicious node. Otherwise, report is trusted and accepted. By MRA scheme, EAACK can detect malicious nodes even in the presents of false misbehavior report. Fig 6 shows the system flow diagram of EAACK scheme.

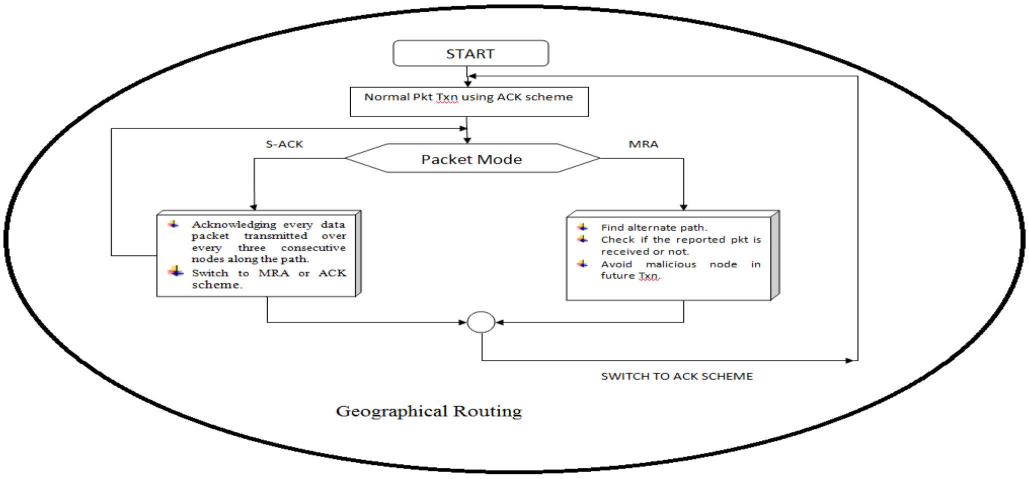
START
Normal Pkt Txn using ACK scheme
S-ACK
Packet Mode
MRA
Acknowledging every data packet transmitted over every three consecutive nodes along the path.
Switch to MRA or ACK scheme.
Find alternate path.
Check if the reported pkt is received or not.
Avoid malicious node in future Txn.
SWITCH TO ACK SCHEME
Geographical Routing

Fig 6 System Flow Diagram

DOI: 10.15680/ijircce.2015.0305165

Geographical Random Forwarding

In normal packet transmission each node has some knowledge of its own position and of the position of the sink node, i.e., the node where the information needs to be delivered. Geographic routing has become one of the most suitable routing strategies in wireless mobile ad-hoc network mainly due to its scalability.

In this research I include a technique for energy efficient and low interference topology control in EAACK was developed in the form of the SBYaoGG algorithm. The SBYaoGG algorithm is a variation of the standard Yao Gabriel graph in which the boundaries of the regions of the Yao graph depend on the distribution of neighbors around a node. The average unit direction vector of the neighbors of a node is used as the axis of the first cone of the Yao graph. The SBYaoGG looks to develop as sparse a topology as possible with good power spanner properties. This is achieved by computing a Gabriel Graph from the original Uniform Disk Graph and then computing the Yao Graph on the Gabriel Graph using smart region boundaries. By this method we can reduce the routing overhead and energy loss with high security.

IV. PERFORMANCE EVALUATION

In this section, we present the result of the simulation. Our example MANET consists of 52 mobile nodes and one base station node. Nodes are randomly distributed in the area. The AODV (AD-Hoc on Demand Distant Vector) routing protocol is used for routing packets in Ideal network.

Fig. 7 shows the effect of EAACK protocol in the attack effected network and GERAF with EAACK in presence of attackers And the Ideal Network in terms of delay. The red line shows the graph for Ideal network transmission scenario and green line shows the effect after implementing attack in ideal network. Blue line shows the EAACK protocol and yellow line shows the graph for Geographical routing with EAACK. From the graph we can see that the delay is reduced considerably after implementing GERAF with EAACK.

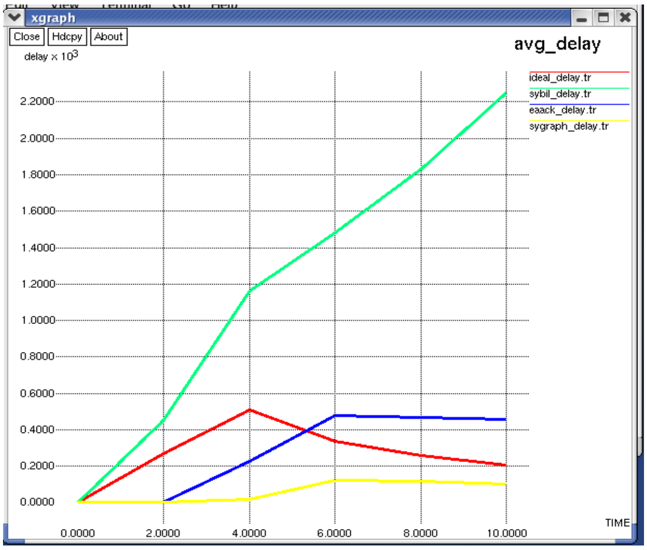

Fig 7 Comparison of delay in 4 situations

Fig. 8 shows the effect of EAACK protocol in the attack effected network and GERAF with EAACK in presence of attackers And the Ideal Network in terms of energy. The red line shows the graph for Ideal network transmission scenario and green line shows the effect after implementing attack in ideal network. Blue line shows the EAACK protocol and yellow line shows the graph for Geographical routing with EAACK. From the graph we can see that the energy is reduced considerably after implementing GERAF with EAACK.

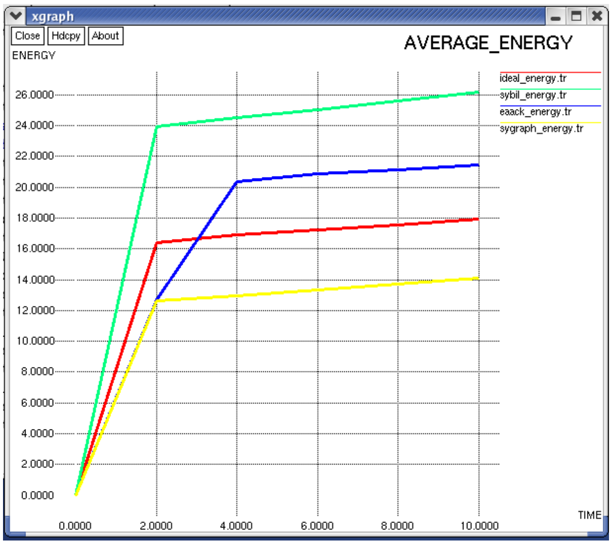

Fig 8 Comparison of energy in 4 situations

Fig. 9 shows the effect of EAACK protocol in the attack effected network and GERAF with EAACK in presence of attackers And the Ideal Network in terms of Packet delivery ratio. The red line shows the graph for Ideal network transmission scenario and green line shows the effect after implementing attack in ideal network. Blue line shows the EAACK protocol and yellow line shows the graph for Geographical routing with EAACK. From the graph we can see that the packet delivery ratio is improved considerably after implementing GERAF with EAACK.

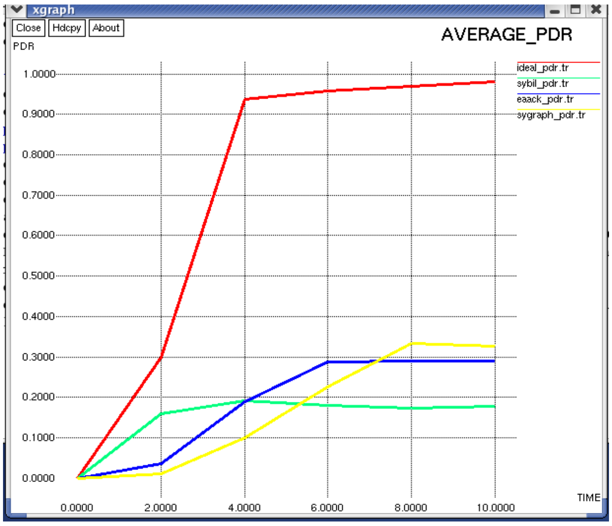

Fig 9 Comparison of delay in 4 situations

Fig. 10 shows the effect of EAACK protocol in the attack effected network and GERAF with EAACK in presence of attackers and the Ideal Network in terms of throughput. The red line shows the graph for Ideal network transmission scenario and green line shows the effect after implementing attack in ideal network. Blue line shows the EAACK protocol and yellow line shows the graph for Geographical routing with EAACK. From the graph we can see that the throughput is reduced considerably after implementing GERAF with EAACK.

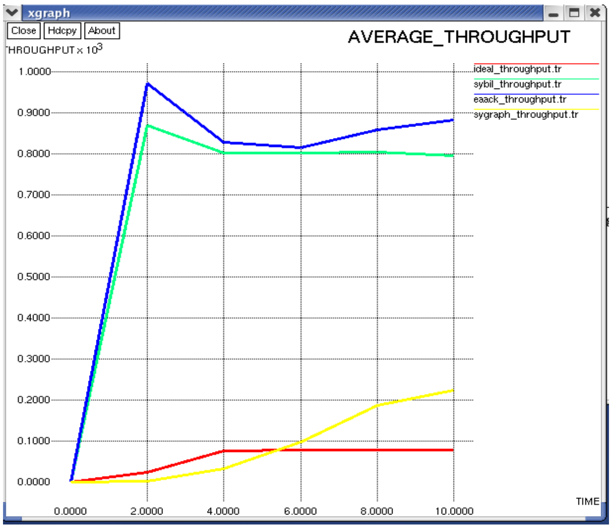

Fig 10 Comparison of delay in 4 situations

V. CONCLUSIONS

In the proposed system, named GERAF with EAACK is an improved version of IDS for MANET. Compared to our previous IDS, GERAF with EAACK provide more efficiency in energy usage and less overhead in routing. When we consider the consequences of group of smart attackers, the entire network may break down. In the future, we plan to investigate on this weakness.

VI. ACKNOWLEDGEMENT

This work has guidance of Mr. Deepak Prasad, Engineer at Punjab National Bank.

REFERENCES

1. 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.
2. 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.
3. 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.
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. 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.
6. 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.
7. 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.