Anomaly Detection System in a Cluster Based MANET

Vikram Narayandas, Sujanavan Tiruvayipati, Madusu Hanmandlu and Lakshmi Thimmareddy

Abstract This chapter presents the development of anomaly detection system (ADS) for locating a malicious node in a cluster based Manet. ADS makes use of AODV protocol that performs route discovery and data forwarding. Each node responds to root request (RREQ) messages and sends root reply (RREP) messages back to the source node. In a cluster based topology a threshold is applied to see if this root reply number is more than the threshold value. If so the node is malicious. Then each node sends an alert to the cluster head (CH) and its neighboring nodes. The proposed ADS avoids the routing to a malicious node thereby preventing high energy consumption of the associated nodes and safeguarding the data transfer in the Manet.

Keywords Manet · ADS · Cluster head · AODV · Energy discharge

1 Introduction

It is challenging to design routing protocols for Mobile Adhoc Networks (MANETs) because of their dynamic topologies and limited resources. Owing to open medium, dynamic topology and lack of central monitoring, Manets are more vulnerable to attacks like denial of services, black hole, gray hole and eavesdropping attacks. The transmission range of each node is limited. Thus, each node needs

V. Narayandas (✉) · S. Tiruvayipati · M. Hanmandlu · L. Thimmareddy
Department of Computer Science & Engineering, MVSR Engineering College, Nadergul, Hyderabad, Telangana, India
e-mail: vikramn_cse@mvsrec.edu.in

S. Tiruvayipati
e-mail: sujanavan_cse@mvsrec.edu.in

M. Hanmandlu
e-mail: hanmandlu_cse@mvsrec.edu.in

L. Thimmareddy
e-mail: tlakshmi_cse@mvsrec.edu.in

S.C. Satapathy et al. (eds.), *Computer Communication, Networking and Internet Security*, Lecture Notes in Networks and Systems 5,
DOI 10.1007/978-981-10-3226-4_2

to perform routing and transmit data packets from one node to others. The misbehaving nodes called attackers in an adhoc network are controlled by adversaries. They try to intrude the network with an intention to cause harm but are also capable of altering the data transfer between different nodes and make the packets difficult to reach their destination [1, 2].

The remainder of this chapter is organized as follows. The related works on Intrusion Detection System (IDS) in Manet are presented in Sect. 2. An overview of AODV and attacks in AODV are discussed in Sect. 3. Section 4 presents the proposed scheme and the derivation of the essential parameters for node description in Manet, and performance metric in routing. The simulation results of the proposed scheme are discussed in Sect. 5. Section 6 gives the conclusions followed by the future work.

2 Related Work

Wireless adhoc networks are configured as flat or multi layered network infrastructure. In a flat network, all nodes are equal but multi layered networks nodes can be considered as clusters with one CH for each cluster [3]. We have already several IDS [4] for Manets like standalone IDS architecture, distributed and cooperative IDS [5]. According to the distributed and cooperative wireless adhoc networks proposed by Zhonge and Lee [6], each node runs as IDS agent and makes local detection decision independently within radio range, here all nodes co-operate in decision making for global detection. Hierarchical IDS [7] is designed for multi-layered adhoc networks. This network is divided into clusters with a CH for each cluster that acts as a manage point similar to switches, routers or gateways. Zone based IDS Adhoc network [1] is partitioned into non-overlapping zones geographically.

3 AODV (Adhoc On-Demand Distance Vector)

AODV [2] used in wireless adhoc networks is capable of both unicast and multicast routing. AODV broadcasts HELLO messages to its neighbors in a network and it has two functions, viz. route discovery and route maintenance from Dynamic Source Routing (DSR) and uses hop-by-hop routing with a sequence number and the periodic beacons from Destination-Sequenced Distance-Vector (DSDV). AODV minimizes the number of required broadcasts by creating routes only on symmetric lines with different phases: (1) Path discovery, route maintenance and (2) Data forwarding. When a source node desires to send a message and initiates a path discovery process to locate its corresponding Mobile host; it broadcasts the route request (RREQ) packet to its neighbors and this request is forwarded to destination via successive neighbors. AODV utilizes a destination sequence number

to ensure that all routes are loop free and contain the most recent data. Each node maintains its own sequence numbers as well as broadcast Id, which is incremented for every RREQ. Once RREQ reaches a destination with fresh route then destination node responds by uni casting route reply (RREP) packet back to the neighbor from which it first received RREQ. On receiving another request the RREQ message is discarded. When a source receives RREP message, link is established between the source node and the destination node. When the receiving node detects the disconnection of route between source node and destination node it generates a route error message (RERR) and sends it to source node. Now source node checks table whether it is in a route map or not. The result is sent to the neighboring nodes in a cluster network.

Types of attacks. The malicious node can misuse AODV [3] by forging source IP address, destination IP address, RREQ, sequence number and hop count. RREQ carries a fresh route in the adhoc network and based on this each node decides whether to forward an RREQ message to the next receiving node until it reaches the destination. The RREQ message is broadcast to select a new route in Manet. If a malicious node sends an excess number of RREQ messages, [8] then the network traffic will become congested with huge amount of RREQ traffic. This congestion leads to delays and packet drops [9]. To avoid this and to identify an excess number of RREQ messages sent by malicious node we go in for ADS. If there is a congestion in RREQ traffic, the neighbor node sends true positive alert to each neighbor and sink node (cluster head) in a cluster network. Each node encounters the traffic RREQ messages sent by source node and records the number of packets in an interval of time [10].

Objective. We focus on detecting the misbehaving nodes that participate in the route discovery and maintenance. To safeguard the data transmission from the onslaught of the misbehaving nodes in the adhoc networks the Anomaly detection method is applied on each cluster having fixed radius.

4 The Proposed Method

Different types of attacks are considered by the authors and an effort is made to quantify denial-of-service (DOS) attacks according to node density, mobility, and system size [11]. The behavior of malicious nodes committing in black hole attack in different routing algorithms like AODV and DSR is studied in [12]. AODV is an efficient protocol but is vulnerable to many security attacks [13]. When traffic is intrusion-prone false alarms are treated as one of the problems that IDS is facing in Manets [6]. Different secure schemes are in vogue to enhance the security in Manets [14, 15] that use Adhoc routing protocols. In the proposed scheme, we detect a malicious node clashing with other activities and frequently sending false RREQ. As a result, malicious node can drop packets for disturbing the working of a routing protocol by IDS. Malicious node may perform different types of attacks like, routing disruption attacks, resource consumption attacks, energy consumption

attacks, passive attacks and active attacks [16]. For each cluster, a cluster head (sink node) is elected based on some quality of service (QOS) Criterion like highest battery power. All nodes send information periodically to the CH. Each node runs its own ADS and sends report to the cluster head and communication takes place subject to the node density and mobility. In the proposed system, we have used ADS for each cluster having a fixed radius. Anomaly Detection system is a process of detecting abnormal activities in a Manet. Major requirements for anomaly detection are depend on high True positive and True positive Rate.

Anomaly Detection system(ADS): An ADS defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. In anomaly IDS even when the traffic signature is unknown, the abnormality can be recognized. Major requirements for anomaly detection are based on high true positive. The true positive (TP) occurs when IDS raises true alerts in response to the detected malicious traffic comprising the total number of detected malicious activities.

Node description: Nodes consume energy while transmitting beacon signals to neighbor's nodes and listen to broadcast messages from neighbor nodes. When forwarding a RREQ message, each node keeps the destination IP address and the sequence number in its routing table. When an RREP message is received, the node checks the Routing table list for the presence of the same destination IP address; if so the sequence number is calculated, and this approach is implemented for every received RREP message to the destination. These nodes are expected to wait for predefined time t, between successive transmissions. Let node 1 start its transmission at time t_1 and reach to another node 2 at time t_2, then the time interval is $\Delta t = t_2 - t_1$. The average of all differences is calculated for each time slot Δt. Each node observes its own traffic and uses a time slot to record the number of packets for each time interval only once when RREQ is received by each receiving node. A Minimum value [17] for the time slot is preferred, and therefore, $\Delta\tau$ is set to a constant which is decided over several time intervals [18]. If RREQ is modified by any malicious node then it tries to send more RREQ messages continuously to the next hop node or other nodes in different time intervals. This is a sign of abnormality in the network. Next the average value is calculated for each time interval Δt [19]. Each node now snaps the connection to the malicious node and avoids the forwarding of the packets to that node. Transmission range can be calculated between two nodes as $\Delta d = d_{max} - d_{min}$. Receiving range can be calculated as $\Delta R = R_{max} - R_{min}$. Power can be calculated as the energy required to forward a packet to the next node as $E_c = E_i - E_{l,}$

Detection of malicious node: A node that sends RREP greater than a threshold of 2 and if energy discharge falls down rapidly then it is said to be malicious. If different networks are considered then threshold should be adjusted as per the network energy discharge and packet delivery parameters.

Pseudo code of the proposed algorithm

```
  while(route_request(node[i]) && node[i](energy[i])>0) {
   cluster_head=highest_energy(node[i]); set_threshold(value);
    if(node[i](rrep[i])>threshold(value)) {
       send_alert_to_cluster_head(node[malicious]);
       send_alert_to_neighboring_nodes(node[malicious]); }
       if(node[malicious]) {avoid_routing(node[malicious]);}
       }
send_packet(); calculate_energy_discharge(); }
```

Different routing parameters in Manet are: packet delivery ratio (PDR), Routing overhead, throughput, end to end delay. Packet delivery ratio (PDR). The number of packets received by the destination to the number of packets sent by a source is PDR = (TR − TS). where, TR is receive time, TS is sent time. Routing overhead = Route discovery + Route maintenance, where Route discovery = RREQ + RREP.

5 Experimental Results

5.1 Simulation Scenario

In our simulation using NS-2, the nodes of a network are grouped into a cluster comprising 1000 × 1000 in a random topology. A cluster head (access point) is elected for the cluster based on the energy parameter. In the cluster topology every node monitors its neighboring nodes and selects a threshold value based on RREQ for sending information to the neighbors. When RREQ exceeds this threshold, then the neighbor node is considered to be a malicious node and the neighboring node of ADS sends a True positive (TP) alert to its neighbors and CH. Each node then avoids the route path to the malicious node. CH is installed for each cluster and the primary objective of CH is to monitor communication between the trusted nodes within a cluster or beyond another CH of the neighbor cluster. ADS is used to detect the abnormal activities in a cluster network and between the clusters in a Manet.

During the cluster anomaly detection, the CH rotates while processing the workload among the neighboring nodes. It detects the routing attacks and monitors a large part of the network activity decision. CH equipped with the knowledge of all clusters has a bidirectional connectivity via a pair of unrelated unidirectional links. When a source has no route to destination, it forwards route request (RREQ) packet

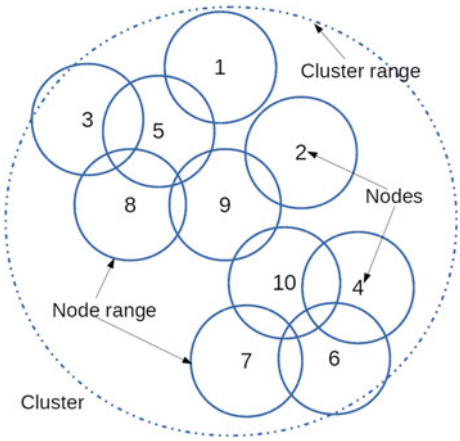

Fig. 1 Cluster setup for simulation

to the CH, When a CH receives request, it appends a request packet to its ID as well as a list of adjacent clusters and rebroadcasts it. A neighbor node also acts as a CH which is a gateway to one or more adjacent clusters and it makes a unicast request to the appropriate CH. Our simulation involves 10 nodes configured into a single cluster having a CH (sink node) dynamically varying based on the energy parameters as shown in Fig. 1. We have used AODV routing protocol for route discovery and route maintenance by hop-by-hop routing with a sequence number and grouped 10 nodes into a single cluster. The energy required for route request (RREQ) is ERREQ and route reply (RREP) is ERREP. The energy discharge of each node is calculated using the energy coefficients of ERREQ and ERREP as $E_{discharge} = E_{coef}$ $(E_{RREQ} + E_{RREP})$. Energy remaining after each node forwards packets to its neighboring nodes is calculated as $E_{remaining} = E_{initial} - E_{discharge}$. Our simulation tests check energy discharge after node delivers its packets to other neighbor nodes at each instance. The energy remaining at an instance "i" for a node is calculated as

$$E(i)_{remaining} = \sum_{1}^{i} E(i-1)_{remaining} - E(i)_{discharge} \tag{1}$$

Substituting for the second term in the LHS of Eq. (1), we get

$$E(i)_{remaining} = \sum_{1}^{i} E(i-1)_{remaining} - \left(E(i)_{coef}\left(E(i)_{RREQ} + E(i)_{RREP}\right)\right) \tag{2}$$

The total energy remaining for all nodes at an instance "i" is

Table 1 Initial node configuration details

Nodes	Initial energy (mAh)	Energy discharge per minute (mAh)	Nodes in range	RREPs per RREQ
1	1000	1	1	1
2	1500	1	1	1
3	2000	1	2	1
4	2500	1	2	1
5	3000	1	3	1
5	3500	1	3	1
7	4000	1	4	1
8	4500	1	4	2
9	5000	1	4	2
10	5500	1	4	3

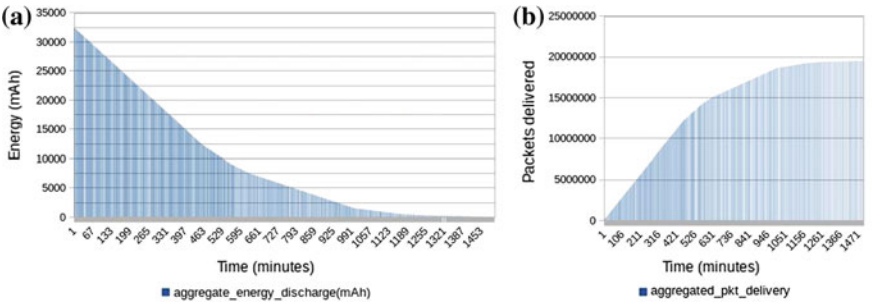

Fig. 2 **a** Aggregate energy discharge of 10 nodes lasting a time of 1500 min, **b** aggregate packets delivered by 10 nodes over period of 1500 min

$$E(n)_{remaining} = \sum_{1}^{n} \sum_{1}^{i} E(i-1)_{remaining} - \left(E(i)_{coef} \left(E(i)_{RREQ} + E(i)_{RREP} \right) \right) \quad (3)$$

Our simulation consists of 3 tests each with its initial node configuration details and energy left after packet delivery and simulated with modal cluster, with and without malicious node, and cluster using ADS with malicious node.

Table 1 gives the simulation results of 10 nodes of different initial energy values along with their discharge per minute (in mAh), nodes in the range 1–4 and RREPs per RREQ for each node is considered with threshold value of 1. Based on the above configuration parameters tests are conducted.

Test-1. Modal cluster without malicious node. When a malicious node is not present i.e. in the secured environment then the energy is least consumed with the highest throughput (packet delivery) as in Fig. 2.

Simulations indicate how nodes consume energy during the packet delivery. The aggregate energy discharge of 10 nodes lasting 1500 min is shown in Fig. 2a.

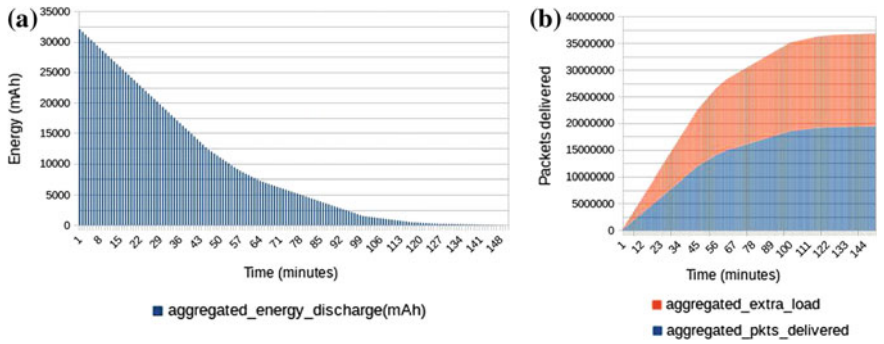

Fig. 3 **a** Aggregate energy discharge of 10 nodes lasting a time of 150 min, **b** aggregate packets delivered by 10 nodes over period of 150 min (color online)

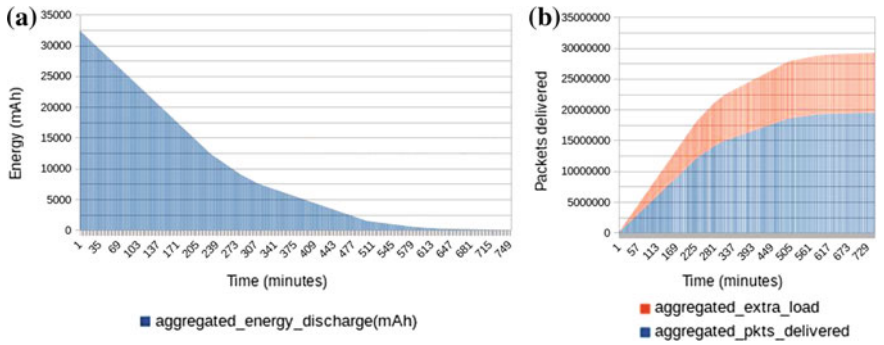

Fig. 4 **a** Aggregate energy discharge of 10 nodes lasting a time of 750 min, **b** aggregate packets delivered by 10 nodes over period of 750 min (color online)

The packets are delivered by 10 nodes over a period of 1500 min. The energy consumed during the packets delivery is shown as the aggregate in Fig. 2b.

Test-2. Cluster with malicious node. In real time when a malicious node is present in the unsecured environment with the unknown neighbors and no ADS then the energy is highly consumed with the lowest throughput (packet delivery). The aggregate energy discharge in a cluster is shown in Fig. 3a. Simulation results display the consumption of energy by the nodes in Fig. 3b, during the packet delivery in a cluster in the presence of malicious node.

Test-3. Cluster with malicious node along with ADS. In the real time situation involving a malicious node the results of energy consumed and throughput (packet delivery) obtained using the ADS are now discussed. The aggregate energy discharge of 10 nodes lasting for 750 min is shown in Fig. 4a.

The simulation results arising out of the ADS show how nodes consume their energy during the packet delivery in a cluster in the presence of a malicious node. The additional and aggregate packets delivered by 10 nodes over a period of 750 min is shown in Fig. 4b.

5.2 Summary of Results

The simulation results of all tests considering the cluster up-time, packets delivered and additional overhead are given in Table 2.

The energy discharged when a cluster node is in the normal mode (test-1) is low. Test-2 shows the energy consumption when a malicious node is present in a cluster. When the nodes are not authenticated the energy discharge is very high. Test-3 shows the real time situation around a cluster node in the presence of the ADS and malicious node. In this case the energy discharge is not so high. A comparison of all tests is shown in Fig. 5. In the past many detection techniques were proposed [4, 8, 16, 20, 21] relating the threshold and activity parameters. Though the statistical analysis of these parameters is made but the energy that plays a major role is ignored in the analysis. In the present work the effect of energy utilization during the conduction of three tests is shown to maintain the cluster energy and also the cluster up time.

Table 2 Simulation results for all tests

Simulation scenarios	Cluster up-time (min)	Packets delivered	Additional overhead
Test scenario-1	1500	19,494,000	0
Test scenario-2	150	19,392,000	17,452,300
Test Scenario-3	750	19,439,200	9,744,600

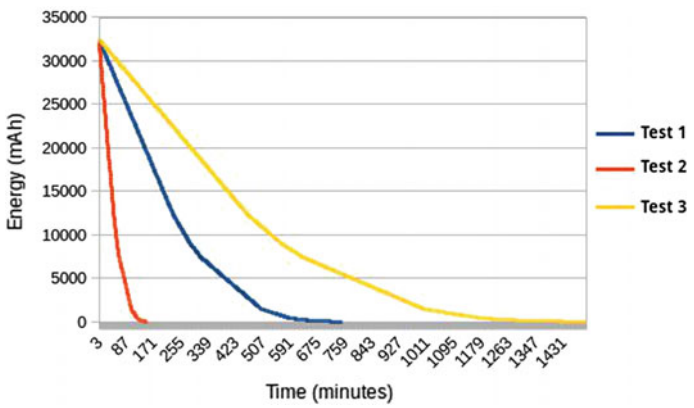

Fig. 5 Comparison of energy discharge for all three tests (color online)

6 Conclusions

The proposed Anomaly Detection System (ADS) is designed to disambiguate all kinds of attacks by detecting a malicious node. The attacks perpetrated one way or the other emanate due to the presence of malicious node. The activities of various attacks can be mirrored through the malicious node. The proposed ADS is demonstrated on a single cluster based topology with 10 nodes. Regarding the simulations, test-1 is concerned with a modal cluster and test-2 centers around a malicious node and test-3 represents real time situation comprising a malicious node and the ADS. The difference in the performance of test-2 and test-3 shows up as a huge difference in the energy discharge and throughput because of the activation of the ADS which dissuades the packets to a malicious node. By this the routing parameters of Manet such as PDR, routing overhead, throughput and end to end delay, are improved drastically. The extent of energy utilization and detection of malicious node during three tests help in keeping the steady discharge of the cluster energy and the cluster up time for a longer period. Further work is on to make the Manets intelligent so that ADS can function much more effectively.

References

1. Y. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless ad hoc networks”, Proc. INFOCOM’ 03, IEEE, San Francisco, CA, April 2003, pp. 1976–1986.
2. L. Zhou, Z. J. Haas, “Securing ad hoc networks”, IEEE Network, Nov/Dec 1999, pp 24–30.
3. H. Deng, R. Xu, J. Li, F. Zhang, R. Levy, W. Lee, “Agent based Cooperative Anomaly Detection for Wireless Ad Hoc Networks,” in Proc. the IEEE Twelfth International Conference on Parallel and Distributed Systems (ICPDS’06),2006.
4. C. Perkins, E. Belding-Royer, and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, Jul. 2003. IETF RFC 3561.
5. Liy.weij “Guidelines on selecting intrusion detection method in manet” 2004.
6. M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz,“On the effect of node misbehavior in ad hoc networks,” in Proc. IEEE Global Telecommun. Conf. GLOBECOM, Jun. 2004, pp. 3759–3763.
7. A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Wireless Commun., vol. 11, no. 1, pp. 48–60, Feb. 2004.
8. Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad-Hoc Networks”, Proc. MOBICOM 2000, Boston, ACM press, pp: 275–283, 2000.
9. Fu, Yingfang; He, Jingsha; Li, Guorui, “A Distributed Intrusion Detection Scheme for Mobile Ad Hoc Networks”, IEEE Computer Software and Applications Conference, 2007. COMPSAC 2007 - Vol. 2. 31st Annual International Volume 2, Issue, 24–27 July 2007 Page(s):75–80.
10. B. Sun, K. Wu and U. Pooch, “Alert Aggregation in Mobile Ad-Hoc Networks” ACM Wireless security (WISE.03), SanDeigo, CA, pp. 69–7.
11. ZaputeN “securing adhoc routing protocols” in ACM workshop on wiress security, USA 2002.
12. Eskin. E, Portray L “A Geometric framework for unsupervised anomaly detection intrusins in unlabelled data” in 2002.

13. Kimay sanzgiri, Daniel laflamne bridget dahil, clay shields and Elzabeth belding Royer "Authentication routing for adhoc networks" IEEE journal on selected areas in communications, vol 23, March 2005
14. C. Perkins, E. Belding-Royer, and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, Jul. 2003. IETF RFC 3561 (Experimental).
15. M. Zapata, Secure ad hoc on-demand distance vector (SAODV) routing, Sep. 2006. IETF Internet Draft, draft-guerrero-manet-saodv-06.txt.
16. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" IEEE Transaction on Vehicular Technology, vol. 58, NO. 5, June 2009.
17. Y. Huang, W. Fan, W. Lee, and P. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in Proc. 23rd ICDCS, May 2003, pp. 478–487.
18. Y. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in Proc. 7th Int. Symp. RAID, Sep. 2004, pp. 125–145.
19. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" IEEE Trans. On Vehicluar Technology, Vol. 58, No. 5, June 2009.
20. P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," in Proc. 4th Annu. IEEE Inf. Assurance Workshop, Jun. 2003.
21. Y. Waizumi, Y. Sato, and Y. Nemoto, "A network-based anomaly detection system using multiple network features," in Proc. 3rd Int. Conf. WEBIST, Mar. 2007, pp. 410–413.

http://www.springer.com/978-981-10-3225-7

Computer Communication, Networking and Internet Security
Proceedings of IC3T 2016
Satapathy, S.C.; Bhateja, V.; Raju, K.S.; Janakiramaiah, B. (Eds.)
2017, XXXI, 623 p. 317 illus., Hardcover
ISBN: 978-981-10-3225-7