Journal of Computer Science 7 (4): 505-511, 2011
ISSN 1549-3636

An Improved Location aided Cluster Based Routing Protocol with Intrusion Detection System in Mobile Ad Hoc Networks

[1]S. Mangai and [2]A.Tamilarasi
[1]Department of Electronics and Communication Engineering,
Velalar College of Engineering and Technology, Thindal, Erode, Tamilnadu, 638 012, India
[2]Department of Computer Science and Engineering,
Kongu Engineering College Perundurai, Erode, Tamilnadu, 638052, India

Abstract: Problem statement: Routing and security are the main challenges for ad hoc networks due to dynamic topology as well as resource constraints. A designed protocol must provide scalable routing with better security. Lack of any central coordination and shared wireless medium makes them more vulnerable to attacks than wired networks. And also resource constraints such as limited energy and size also play an important role in the protocols designed for security. **Approach:** In this study, Improved Location aided Cluster based Routing Protocol (ILCRP) for GPS enabled MANETs was analysed in MANETs with malicious nodes and an Intrusion Detection System was used to increase the packet delivery ratio. ILCRP makes use of location aided routing in the presence of cluster based routing Protocol. **Results:** Use of location information with security against attacks results in high packet delivery ratio for the cluster based routing protocol. Simulations are performed using NS2 by varying the number of nodes. **Conclusion:** The results illustrate ILCRP provides higher delivery ratio with IDS.

Key words: Routing algorithm, location aided routing, cluster based routing, intrusion detection system, routing protocol, dynamic topology, cluster head, packet delivery ratio

INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous system of mobile stations connected by wireless link to form a network. It does not rely on predefined infrastructure to keep the network connected therefore it is also known as infrastructure less networks. In MANET, each node can communicate with node in its range and those which are beyond the range can communicate using the concept of multi hop communication. These networks are particularly useful and well suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery. In the MANET the network topology may change rapidly and unpredictably. Due to their dynamic topology, the network is highly prone to attacks. So the functioning of the Ad hoc network depends on the trust and cooperation between nodes.

The need for routing protocols with minimum overhead combined with coping with large node density (scalability) (Natsheh and Buragga, 2010) emphasis the use of clustered structure for MANETs. Clustering offers five outstanding advantages over other protocols. First, it uses multiple channels effectively and improves system capacity greatly. Second, it reduces the exchange overhead of control messages and strengthens node management. Third, it is very easy to implement the local synchronization of network .It provides Quality of Service (QoS) routing for multimedia services efficiently .Finally, it can support the wireless networks with a large number of nodes.

Achieving security within ad hoc networks is very difficult because of the following reasons (Gunasekaran and Doraiswamy, 2010):

- Dynamic topology
- Open and Vulnerable Media
- Roaming in Dangerous Environment

When operating in hostile or suspicious settings, MANETs require communication security especially in underlying routing protocols. As a result, attacks with malicious intent have been and will be devised *to exploit* these vulnerabilities and *to cripple* the MANET operation. In general the attacks are classified into two types passive attacks and active attacks.

Corresponding Author: S. Mangai, Department of Electronics and Communication Engineering,
Velalar College of Engineering and Technology, Thindal, Erode, Tamilnadu-638 012, India

Passive attacks is eavesdropping only, but not endangering message transmission. Active attacks are more severe. Active attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. For this reason, there is a need of second mechanism to "detect and respond" to these newer attacks, by an effective "Intrusion Detection System (IDS)"as a second line of defense.

Intrusion Detection System is defined as the method to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". It is pertaining to techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. The Intrusion detection System monitors the activities of the system, analyze the activities to determine that any of the activity is violating the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity (Anantvalee and Wu, 2007).

MATERIALS AND METHODS

Intrusion Detection Systems (IDS): Intrusion Detection Systems are designed to enhance fact finding operations in computer systems, the goal is to help accomplish the task of searching and detecting of attacks by collecting related information from a variety of system and network sources, thereafter analyzing the collected information for symptoms or traces of security disorders. The IDS provides the following functions:

- Auditing of system configurations and vulnerabilities
- Monitoring and analysis of user and system activities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating system audit trial management with recognition of user reflecting policy violations

Intrusion Detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets form network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows:

In misuse based Intrusion Detection System also called signature based detection, a pre-written rule or pattern is used to match an attack. The system compares the captured data with these profiles and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initiating a proper response.

In anomaly based IDS, normal profiles (or normal behaviors) of users are kept in the system and then the captured profile is compared with these profiles. If IDS found any activity that deviated from the normal profile then that activity is detected as anomaly.

In Specification based IDS, some set of constraints are defined for correct operation of program and then operations are monitored against these defined constraints. A mismatch is reported as an attack.

Intrusion Detection in MANETs: Many intrusion detection systems have been proposed in traditional wired networks, where all traffic must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily (Syurahbil *et al*., 2009). On the other hand, MANETs do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated information. Thus, the current IDS techniques on wired networks cannot be applied directly to MANETs. Many intrusion detection systems have been proposed to suit the characteristics of MANETs, some of which will be discussed in the next sections.

Architectures for IDS in MANETs: The IDS architecture for a wireless ad hoc network may depend on the network infrastructure itself. Wireless networks may be configured in either flat or multi-layered network infrastructure. In a multi-layered network infrastructure, all nodes are considered heterogeneous, while in a flat network infrastructure, all nodes are considered homogenous (equal and may participate in routing functions) .The IDS can be classified into three categories which can be adjusted and suited for MANET.

Stand-alone IDS: In this architecture the IDS runs on each node independently to determine intrusions. There is no cooperation and no data exchanged among the IDS's on the network. This architecture is also more suitable for flat network infrastructure than for multilayered network infrastructure (Sun *et al*., 2007).

Distributed and Cooperative IDS: This IDS has a rule that every node in the MANET must participate in the Intrusion Detection and respond by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.

Hierarchical IDS: It is an extended version of the distributed and cooperative IDS architectures. This architecture proposes for multi-layered network infrastructures where the network is divided into clusters with each cluster controlled by a cluster head. Here each IDS agent is run on every member node and is responsible locally for its node, i.e., monitoring and deciding on locally detected intrusions. A cluster head is responsible locally for its node as well as globally for its cluster, e.g. monitoring network packets and initiating a global response when network intrusion is detected (Zhang *et al*., 2003).

"Watchdog and Path rater" scheme is used to detect and mitigate the effect of nodes that do not forward packets. Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped, match with the observing node's buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified.

Knowledge-based intrusion detection systems was proposed by H.Y. Chang, S.F. Wu and Y.F. Jou, which accumulate knowledge about attacks, examine traffic and try to identify patterns indicating that, a suspicious activity is occurring. This approach can be applied against known attack patterns only and the utilized knowledge base needs to be updated frequently.

K.Paul and D.Westhoff proposed a approach that uses hash chain in route discovery process and an observer to detect the malicious behavior of the neighbor node and then the neighbor reports the behavior of the node to source node which calculates the rating for the accessed node and this rating is used to decide the malicious node but this method is not a pure IDS because it uses a cryptographic mechanism to detect the attacks.

O.Kachirski and R.Guha, proposed a sensor based approach to detect intrusion, in which multiple sensors are deployed and audit data is collected from all the sensors and these data is merged to detect the intrusion .

The zone based Intrusion Detection for MANET introduces a geographic zone based intrusion detection frameworks that uses a location aware zone gateways node to collect and aggregate the alerts from intra-zone nodes.

A cooperative intrusion detection architecture facilitates accurate detection of MANET-specific and conventional attacks. The architecture is organized as a dynamic hierarchy in which detection of data is acquired at the leaves and is incrementally aggregated, reduced and analyzed as it flows upward toward the root. The nodes at the top are responsible for security management functions.

Detecting Intrusion Attacks in MANETs proposed a model which does not perform any change in underlying protocol and used additional security component to detect fabrication attack, resource consumption attack and packet dropping attack.

Collaborative technique for Intrusion detection in MANET (Marchang and Datta, 2008) proposed two intrusion detection techniques for mobile ad hoc networks, which use collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood.

Pasquale Donadio, Antonio Cimmino and Giorgio Ventre proposed a Grid based Intrusion Detection System (G-IDS) that uses the basic principles of the Grid computing and apply them to the intrusion detection mechanisms, in order to define a new process capable to protect networks characterized by the constantly changing of the topology.

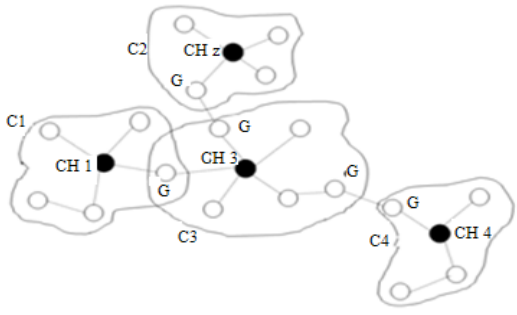

Fig. 1: ILCRP cluster formation

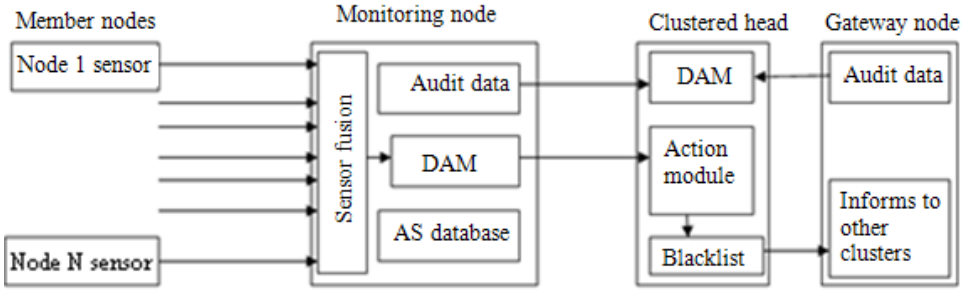

Fig. 2: IDS in ILCRP

Cluster Based Routing Protocol , an on demand source routing protocol, divides clusters into nodes and decreases control overhead during route discovery. K-Hop Cluster Based Routing Protocol (Zang and Tao, 2009) improves CBRP with increase in number of nodes and its mobility. It modifies the existing Weighted Clustering Algorithm (WCA) (Nanni and Basagni, 2010) for the election of Cluster Head.

In Location-Aided Routing (LAR) (Ko and Vaidya, 1998) protocol the overhead of route discovery is decreased by utilizing location information of mobile nodes. Using GPS for location information, LAR protocol reduces the search space for a desired route. Reducing the search space results in fewer route discovery messages. By contacting a location service provider which knows the positions of all the nodes, the source node should first get the position of the destination mobile node when it wants to send data packets to a destination.

To localize the ad hoc network a wide variety of routing protocols (Mikki, 2009; Khatri *et al*., 2010; Vijayaragavan *et al*., 2009) have been proposed over the years. Some techniques use GPS but for very few nodes. These nodes are often referred to as anchor nodes or reference nodes. 'Completely GPS Free Localization or 'Using Very Few Anchor Node' (Chu and Jan, 2007) are the two types of localization approaches that provide techniques to localize the network in a GPS Less or GPS-Scarce area (LACBER). The GPS-less localization approaches establish a virtual coordinate system and try to localize the network in that coordinate System. On the basis of distance measurement (using ToA or AoA or RSSI) or hop count these coordinate systems are established. Using the above coordinate systems the exact location of the node cannot be determined due to absence of GPS.

The ILCRP protocol (Mangai and Tamilarasi, 2010), a stable clustering protocol ,applicable for highly mobile ad hoc networks was proposed earlier where all the nodes in all the clusters are GPS enabled compared to few nodes in a cluster as in LACBER protocol (Deb *et al*., 2009). This protocol makes use of clusters as well as location information intensively as shown in Fig. 1. The exact information of the nodes is known to each other with the help of GPS which increases the packet delivery ratio and reduces the control overhead and makes the route, loop free. Location information of the nodes keeps the exchange information as well as the end to end delay very low.

Clusters are formed between nodes which are m-hops far away from the cluster head. Nodes with highest Node Value is selected as cluster head. Two tables namely Neighbor table and Cluster Adjacency table facilitate the formation and functioning of clusters. The Neighbor table is a conceptual data structure for formation of a cluster whereas Cluster Adjacency Table (CAT) is used for keeping information about the adjacent clusters.

Proposed protocol: The Proposed protocol ILCRP-IDS uses Distributed Cluster based IDS with GPS enabled nodes and it overcomes the problems associated with passive and active attacks by introducing the Intrusion Detection System (IDS).

In ILCRP-IDS ,due to energy constraint the cluster head selects node with a second highest Node Value as in ILCRP as the Monitoring Node of the cluster .It is in the Monitoring node that the IDS is located .This node monitors and captures live packet traffic on the network. All the member nodes of the cluster act as the sensors for the IDS in the cluster. The sensor nodes obtain their audit data (metadata of their transmission as well as the reception of the data) and forward it to their monitoring node of the cluster. The monitoring node's Fusion Module as shown in Fig. 2 combines all the audit data of all the nodes in the cluster to analyze each transmission that occurred in the cluster. Analyzing the audit data, the monitoring node detects any malicious activity in the path of the nodes between the source and

destination node using Detection and Analyzer Module (DAM). The Detector and Analyzer Module (DAM) works according to the following rules

Interval rule: Considering a pre-defined time frame, a failure is observed if the time passed between the receptions of two consecutive messages is larger or smaller than the allowed limits . Integrity rule: Any attack on modification of the transmitted packet within the transmission channel is subject to anomaly and will be detected based on this rule. A propagation failure due to the jammer's interference in the network constitutes example of such rule and will be used as part of our detection process.

Transmission/retransmission rule: Monitoring by the monitor node pertaining to number of messages intended for any of its neighbor's falls below expectancy as the nodes fails to forward the message to the next hop.

Delay rule: The transmission of a message by a monitor's neighbor must occur before a defined time out otherwise an attack will be detected.

Most of the common malicious activity in MANETs are black hole (grey hole), Worm Hole attack, node impersonation.

There may be a possibility that the monitoring node can become malicious node. In order to monitor the activity of the monitoring node, the cluster head detect and analyze the audit data obtained from the monitoring node. If any malicious activity is found on the node, the cluster head replaces with another node and moving the node to blacklist. Cluster head also monitors the activity on the gateway node. There may be another possibility of malicious activity on the cluster head itself whose activities are collectively monitored by all the nodes in the cluster.

A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. Due to continuous monitoring of the transmission and reception of metadata, a node functioning as the black hole can be easily identified and submitted to cluster head for further action. On receiving information from the monitoring node, the cluster head marks that node as the blacklisted node of the cluster and adds it to the blacklist. The cluster head broadcasts the blacklist to all the member nodes of the cluster. The gateway nodes informs the adjacent clusters about the malicious node. Since ILCRP uses the permanent identifier for all node which is the MAC address, the adjacent cluster heads adds the MAC address to their cluster's blacklist.

A wormhole attack is a severe attack on MANET routing where two attackers connected by a high speed off channel link, are strategically placed at different ends of a network. They have the complete control of the link, attackers can drop the packets to be forwarded by their link. They can drop all packets, a random portion of packets or specifically targeted packets. Since exact information of the nodes are known to all the nodes in ILCRP, the wormhole does not exist in the cluster. Node impersonation does not occur due to use of long and permanent identifier for each node.

RESULTS AND DISCUSSION

Simulation parameters:

- Performed using NS-2 network simulator with MANET extensions
- IEEE 802.11 is used as the MAC layer protocol.
- The radio model simulates with a nominal bit rate of 2Mbps
- Nominal transmission range is 125 meters.
- The radio propagation model is the two-ray ground model
- First 100 nodes are deployed for one experiment and then 100 nodes are used for another experiment in a field of 1000m X 1000m
- The traffic pattern is CBR (constant bit rate) with a network traffic load of 4 packet/second and the packet length are 512 bytes
- The mobility model used is the Random Waypoint Model
- The pause time of the node reflects the degree of the node mobility. The small pause time means intense node mobility and large pause time means slow node mobility. The pause time is maintained as 5 seconds
- The simulation time is 900 seconds
- The simulations are performed by creating 20, 40, 60, 80, 100 nodes keeping speed constant to 5 m/s

Performance metrics: For evaluating the performance of ILCRP with Intrusion Detection System, the metrics chosen are Packet Delivery ratio and Control Overhead.

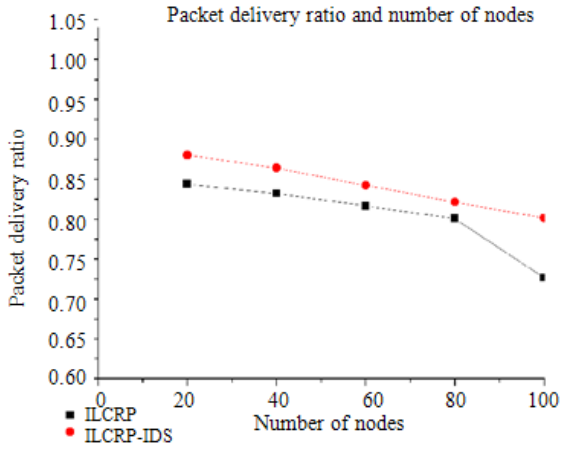

Fig. 3: Comparison for Packet Delivery Ratio and Number of Nodes

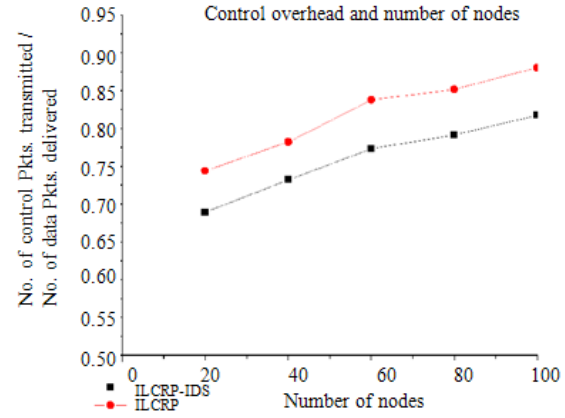

Fig. 4: Comparisons for Control Overhead and Number of Nodes

Packet delivery ratio: It is defined as the ratio of total number of packets that have reached the destination node to the total number of packets originated at the source node. The location information of the nodes make the packets route, loop free which results in high packet delivery ratio. Due to presence of IDS, packet drops due to malicious nodes are reduced which results in higher ratio compared to ILCRP with malicious nodes in clusters. Figure 3 confirms the packet delivery ratio between ILCRP and ILCRP with IDS in clusters with malicious nodes

Control overhead: It is defined as the ratio of the number of control packets transmitted to the number of the data packets delivered. Usage of cluster based routing protocol for clustering and exact location information for route discovery reduces the control overhead in the network. Further with IDS, the control overhead increases with monitoring activity on all nodes by monitoring node as well as cluster head. Figure 4 shows the control overhead ratio between ILCRP and ILCRP with IDS.

CONCLUSION

This study applies the Intrusion Detection System for the ILCRP for clusters with malicious nodes. Even though ILCRP was a stable clustering scheme, it lacks in terms of security attacks. Due to presence of intrusion detection system as well as the exact location information of the nodes are known, It performs better in terms of packet delivery ratio. But Security comes with increase of control overhead. ILCRP is not affected by worm holes due to its location based information but some of the attacks are secured by IDS proposed. Since IDS is performed collectively, the energy consumption is further reduced compared to the consumption if IDS is used per node. Further research on security for ILCRP such as Key Management, Authentication can result in better secured protocol.

REFERENCES

Anantvalee, T. and J. Wu, 2007. A survey on intrusion detection in mobile ad hoc networks. Wirel. Network Secu., 2: 159-180. DOI: 10.1007/978-0-387-33112-6_7

Chu, H.C. and R.H. Jan, 2007. A GPS-less, outdoor, self-positioning method for wireless sensor networks. Ad Hoc Networks, 5: 547-557. DOI: 10.1016/j.adhoc.2006.03.004

Deb, D., S.B. Roy and N.Chaki, 2009. LACBER: A new location aided routing protocol for gps scarce MANET (2009). Int. J. Wire. Mob. Networks, 1: 22-35. http://www.airccse.org/journal/nsa/0809smn02.pdf

Gunasekaran, S. and K. Doraiswamy, 2010. Security challenges in multicast communication for mobile ad hoc network. J. Comput. Sci., 6: 566-571. DOI: 10.3844/jcssp.2010.556.571

Khatri, P., M. Rajput, A. Shastri and K. Solanki, 2010. Performance study of ad-hoc reactive routing protocols. J. Comput. Sci., 6: 1159-1163. DOI: 10.3844/jcssp.2010.1159.1163

Mangai, S. and A. Tamilarasi, 2010. Improved location aided cluster based routing protocol for GPS enabled MANETs. Future Gen. Inform. Technol., 6485: 606-615. DOI: 10.1007/978-3-642-17569-5_60

Marchang, N. and R. Datta, 2008. Collaborative techniques for intrusion detection in mobile ad-hoc networks. J. Ad hoc Networks, 6: 508-523. DOI: 10.1016/j.adhoc.2007.04.003

Mikki, M.A., 2009. Energy efficient location aided routing protocol for wireless MANETs. Int. J. Comput. Sci. Inform. Secur., 4: 1-9. http://arxiv.org/abs/0909.0093

Nanni, M.A. and S. Basagni, 2010. Mobile ad hoc backbones: Formation and maintenance. Proceedings of 2010 IEEE Symposium on Radio and Wireless, Jan. 10-14, IEEE Xplore, New Orleans, LA., pp: 613-616. DOI: 10.1109/RWS.2010.5434229

Natsheh, E. and K. Buragga, 2010. Density based routing algorithm for spare/dense topologies in wireless mobile ad-hoc networks. Am. J. Eng. Applied Sci., 3: 312-319. DOI: 10.3844/ajeassp.2010.312.319

Sun, B., L. Osborne, Y. Xiao and S. Guizani, 2007. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wire. Communi., 14: 56-63. DOI: 10.1109/MWC.2007.4396943

Syurahbil, N. Ahmad, M.F. Zolkipli and A.N. Abdalla, 2009. Intrusion preventing system using intrusion detection system decision tree data mining. Am. J. Eng. Applied Sci., 2: 721-725. DOI: 10.3844/ajeassp.2009.721.725

Vijayaragavan, S., K. Duraiswamy, B. Kalaavathi and S. Madhavi, 2009. A performance study of reactive multicast routing protocols in virtual class room using mobile ad hoc network. J. Comput. Sci., 5: 788-793. DOI: 10.3844/jcssp.2009.788.793

Zang, C. and C. Tao, 2009. A multi-hop cluster based routing protocol for MANET. Proceedings of the 2009 1st IEEE International Conference on Information Science and Engineering, (ICISE'09), IEEE Computer Society Washington, DC, USA., pp: 2465-2468. DOI: 10.1109/ICISE.2009.75

Zhang, Y., W. Lee and Y.A. Huang, 2003. Intrusion detection techniques for mobile wireless networks. Wire. Networks, 9: 545-556. DOI: 10.1023/A:1024600519144