# Approaches for Enhancing the Performance and Security of Mobile Ad Hoc Networks

Roopa.M [#1],.Selvakumar Raja.S [*2]
[#1] Research scholar, Sathyabhama University, Chennai, Tamilnadu
[*2]Dean, Arunai College of Engineering, Tiruvannamalai,Tamilnadu

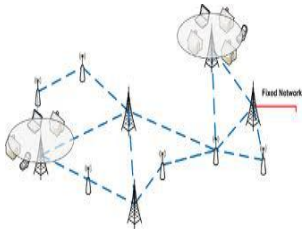
***Abstract*— In past few decades the wired network has been migrated to wireless network. The mobility and scalability of wireless network made it possible in many applications .The next stage of advancement was Mobile Ad hoc network (MANET).**

**As compared to the other wireless networks that need a centralized node, fixed network infrastructure and limited coverage range , a MANET does not require a fixed network infrastructure and there is no limitation in perimeter .Here every single node works as both a transmitter and a receiver. The nodes are self-configuring and communicate directly with each other when they are within the same communication range. Otherwise, they rely on their neighbours to relay messages. The open medium , continuous advertisement by a node ,and wide distribution of nodes make MANET vulnerable to malicious attackers. The nodes act both as routers and as communication end points. This makes the network layer more prone to security attacks. . Also due to the distributed nature the identification of the threats becomes difficult. In this paper a survey is made on- types of attacks , intrusion detection system(IDS) , protection mechanisms , prevention techniques, security solutions and vulnerabilities in MANET to reduce the computational complexity during data communication.**

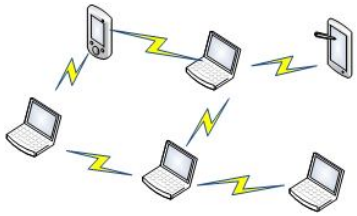
**Keywords— Mobile Adhoc network , Security, IDS**

## I. INTRODUCTION

The improved technology and reduced costs, have made wireless networks gain more preferences over wired networks in the past few decades. The major advantages of wireless networks is its ability to allow data communication between different parties and maintain their mobility. But, this communication is limited to the range of transmitters. That is two nodes cannot communicate with each other when the distance is beyond their own communication range .Also, wireless networks have at least one access point, which is usually connected to a wired network. A central node which is called "base station" or "access point" exists in the network so that all the connections are done through this central node .It uses infrastructure mode .All the above gaps are filled by a MANET network. Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly[2].They are temporary infrastructure less self-organizing and self-configuring network that dynamically establish their own network on the fly. MANETs were initially proposed for military battle field communication applications and currently their use include emergency disaster relief, sensing or controlling a region, sharing information during a lecture or conference. **[3]**




(a)An infrastructured network with base stations.



(b) A mobile ad-hoc network

Figure 1: Infrastructured and ad-hoc networks

## II LITERATURE SURVEY

*The main characteristics of Manet are:*

*1) Distributed operation*: There is no central network for the control operations, the control of the network is distributed among the nodes. Each nodes involved is must cooperate with each other and communicate among themselves. Here each node acts as a relay to provide routing and security.

*2) Multi hop routing*: When nodes are out of range the data is send via intermediate nodes. To send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

*3)Independent terminal*: Each mobile node is an independent node, and functions as both a host and a router.

*4)Dynamic topology*: Nodes move freely with different speeds and the network topology change randomly and at unpredictable time. The nodes create there own network after travelling around.

*5)Less weight nodes*: The nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

*6)Shared Medium*: The physical medium is accessible to any node.The access to the channel is not restricted.

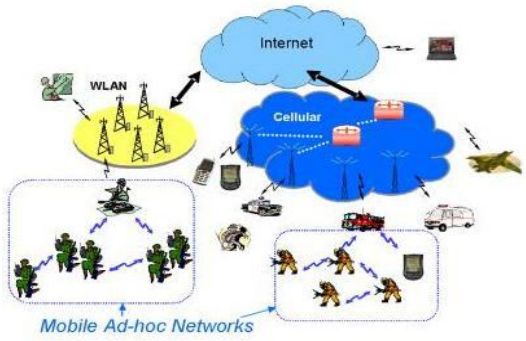



Figure 2 :A simple Manet

*Drawbacks of Manet:*

*1)Reduced bandwidth:*

It has lower capacity than infra structured networks. The throughput is less than maximum transmission rate due to the effect of multiple access, fading, noise, and interference conditions.

*2)Dynamic topology:*
The changing topology disturbs the trust maintained by nodes.

*3)Routing Overhead:*
Due to the frequent change of location within network some false routes are generated in the routing table which leads to unnecessary routing overhead.

*4)Hidden terminal problem:*
Due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver a collision occurs. This is called a hidden terminal problem.

*5)Packet losses:*
The increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes a Ad hoc networks experiences a much higher packet loss.

*6)Dynamic route changes:*
The network topology is highly dynamic as the nodes move. This results in frequent path breaks hence results in frequent route change.

*7)Battery consumption:*
To obtain portability, small size and less weight Used in these networks have power restrictions.The main features of mobile ad hoc network are Unreliability of wireless links between nodes, changing topology and lack of security feature (availability, confidentiality, integrity, authentication, non repudiation) and Resource constraints.

*8)Security:*
As the communication is through wireless medium and transmission is mostly through multiple nodes the networks are intrinsically exposed to numerous security attacks.

9) *Scalability:*
The prediction of nodes is difficult. The characteristics of MANETS pose both challenges and opportunities in achieving security goals**.**

*The different Security Criteria in Manet are:*
*1)Availability:*
The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

2) *Integrity:*
Integrity guarantees the identity of the messages when they are transmitted.

*3)Confidentiality:*
Confidentiality means that certain information is only accessible to those who have been authorized to access it.

*4)Authenticity:*
Authenticity is essentially assurance participants in communication are genuine and not Impersonators.

5) *Nonrepudiation:*
Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message.

6) *Authorization:*
Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

*7)Anonymity*
Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software.

Attack Types in Mobile Ad Hoc Networks

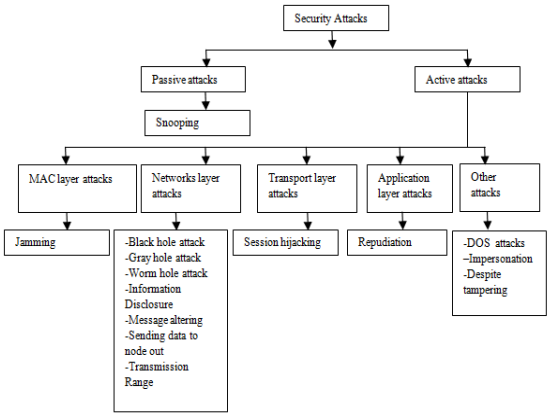



Figure 3:Classification of Attacks

The attacks in MANETS are classified into two major categories, namely passive attacks and active attacks[5].

1)Passive attacks are launched by the adversaries solely to snoop the data exchanged in the network. These adversaries don't disturb the operation of the network. The identification of such attacks becomes very difficult since network itself does not get affected and they can reduced by using powerful encryption techniques.

2)Active attack tries to alter or destroy the information being exchanged, hence disturbing the normal functionality of the network. Attacks can also be classified according to network protocol stacks

As the nodes in ad hoc networks act both as routers and communication end points the network layer are more prone to security attacks. Security is an essential service for network communications.

In this session the attacks in network layer are discussed .The different network layer attacks are:

*Black hole Attack*:

Intruders can exploit the vulnerability in route discovery procedures of on-demand routing protocols, such as AODV and DSR, when a node requires a route towards the destination .The node sends a RREQ and an intruder advertises itself as having the fresh route. By repeating this for route requests received from other nodes, the intruder may succeed in becoming part of many routes in the network. The intruder once chosen as an intermediate node, drops the packets instead of forwarding or processing them, causing a black hole (BH) in the network.

*Wormhole:*

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole [6] . Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

*Grey hole*:

A grey hole attack (GH) is a special case of the BH attack, in which an intruder first captures the routes, that is, becomes part of the routes in the network (as with the BH attack), and then drops packets selectively.

*Byzantine attack***:**

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths ,or selectively dropping packets, which results in disruption or degradation of the routing services.[7]

*Information Disclosure*:

This type of attacks is executed by the compromised nodes in the network by leaking the confidential or important information to the unauthorized nodes in the network.

*Message Tampering*:

This attack is launched by the adversaries acting as compromised nodes during communication. They try to take all the data packets and modify the data that has details about network topology, optimal routes etc; this is done by adding additional bytes or by deleting existing bytes. A small change in the data may obviously cause abnormalities or havoc in the network.

*Routing Attacks*:

1) Packet Replication attack: In this type of attack the adversary replicates the stale packets. This leads to consumption of network bandwidth and battery power of the nodes thereby creating a confusion in the routing process.

2) *Route Cache Poisoning*: Here a compromised node in the network send some fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. This result in sub-optimal routing, congestion in the portions of network or some parts of the network becomes inaccessible.

3) *Rushing attack*: In this attack an adversary takes the RREQ packet from source node and floods the packet quickly to all the other nodes in the network, before they get the same packet from the source. Once the original RREQ packet comes to the nodes, it is assumed as a duplicate one and rejects it since they already have the packet from adversary.

*Multilayer Attack:*

*Denial of Service Attack (DOS):* In this attack adversary tries to prevent all the legitimate and authorized users of the network from the services offered by the network. In network layer this attack is carried by flooding packets through a centralized resource to make it unavailable for all other nodes in the network. This makes failure in the delivery of guaranteed services to the end users.

*Security attacks countermeasures*

The primary concern has became security in order to provide a secure and protected communication between mobile nodes in an open hostile environment. The challenges that are nontrivial make a case for building multi defence security solutions that is able to achieve both broad protection and desirable network performance. The figure shows classification of lines of defence. security mechanisms follow two defence lines: one preventive and another reactive [13]. The former provides mechanisms to avoid any type of attack, as firewalls and cryptographic systems. Cryptographic tools are widely used to provide powerful security services, such as confidentiality, authentication, integrity, and non-repudiation. But, cryptography cannot guarantee availability; for example, it cannot prevent radio jamming. The main requirement to ensure security in MANETS is to have a secure routing protocol which should have properties to detect malicious nodes, guarantee of exact route discovery process, maintaining confidential network topological information and to be self-stable against attacks The latter consists in taking action on demand to mitigate intrusions, as intrusion detection systems (IDS). Nevertheless, preventive and reactive solutions are efficient to put all attacks and intrusions off [14], [15]. Thus, research

groups have built security mechanisms toward one third defence line, called intrusion tolerance (IT) [14].

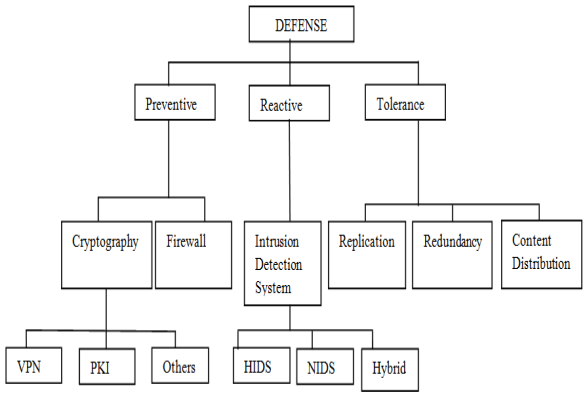



Figure 4: Taxonomy of lines of defense

To preserve node identities and node movements different protocols are used. DSR developed by Johnson and Maltz is widely used protocol considered to be simplest and effective. DSR is a purely on-demand ad hoc network routing protocol. A Secure Route Discovery Protocol (SRDP) is advancement of DSR that works with a range of cryptographic primitives, some based on aggregated MACs and others on digital signatures amenable to aggregation. Privacy-friendly Routing in Suspicious MANETs protocol (PRISM). PRISM[11] is an anonymous location-centric or a identity-centric on-demand routing protocol based on three main building blocks: (1) the well-known AODV routing protocol, (2) any secure group signature scheme (or one time public key certificates), and (3) location information .(AODV)Ad hoc on demand vector routing is a protocol that works for a dynamic self starting network and no periodic routing information is required. AODV is on-demand (reactive) and thus does not propagate topology information, in contrast with proactive protocols, such as OLSR . SPAAR (Secure position aided ad hoc routing)and AO2P (ad hoc on-demand position-based private routing protocol)require on-line location servers. ASR (Anonymous Secure Routing) and ARM (anonymous routing protocol) assume that each authorized source-destination pair pre-shares a unique secret key. DSR(Dynamic Source Routing), EARP (Efficient Anonymous Routing Protocol) and ARMR (Anonymous Routing Protocol With Multiple Routes for communications) assume that each source destination pair shares some secret information, which could be the public key of the destination or a secret key. ANODR (Anonymous On Demand Routing With Untraceable Routes) assumes that the source shares some secret with the destination for the construction of a trapdoor. SDAR (Secure Distributed Anonymous Routing Protocol) assumes that the source knows the public key of the destination, obtained. PRISM is basically different from all other anonymous on-demand MANET routing protocols in two ways: (1)It uses a location-centric rather than a identity-centric, communication paradigm.(2)It requires no pre-distributed pairwise shared secrets and on-line servers. Another development was ALARM[10](Anonymous Location-Aided Routing in Suspicious MANETs)routing protocol. This uses nodes current locations to securely disseminate and construct topology snapshots and forward data. The goals of ALARM were Privacy, Security and Performance.

The basic operation of ALARM is to provide initialization of group signature and enrolls all legitimate MANET nodes as group members . A unique private key and secret key is produced by the node with the knowledge of group manager. Group signature schemes with self-distinction can be used to prevent Sybil attacks, albeit .This provides security and privacy to the network. Sybil attacks can be easily detected offline, if the optional forensics feature is enabled and operational logs are off-loaded to GM for analysis .The ALARM protocol address scalability and insider threat issues. The advantage of the basic ALARM protocol is its simplicity and effectiveness.

*The drawbacks of ALARM are*: 1) Due to flooding, scalability is a problem for large MANETs 2) any node can lie about its location or generate multiple LAMs as part of a Sybil attack.

A second line of defense mechanism is intrusion detection systems (IDS) applied in MANET. IDS are some of the latest security tools in the battle against attacks. An Intrusion Detection System (IDS)detects unwanted manipulations to systems.

Intrusion detection technique, which was developed first in the wired network and had become a very important security solution. IDS can be split into three main classes based on the detection approach employed: (1)anomaly-based intrusion detection (ABID), also known as behaviour-based intrusion detection; (2) misuse detection, also known as knowledge-based intrusion detection (KBID); and (3) specification-based intrusion detection (SBID).

*1) Anomaly-Based Intrusion Detection* : ABID systems are also called as behaviour-based intrusion Detection. Here the model of normal behaviour of the network is extracted, and then this model is compared with the current behaviour of the network to detect intrusion in the network. A diagram illustrating the basic ABID process is shown in Fig.5 . Anomaly detection systems typically consist of two phases of operation: training and testing [16].In training the modelling of the normal or expected behaviour of the network or of the users are performed. The model also acts as a profile of user or network behaviour. A profile has information about the list of parameters which are geared to the target being monitored. ABID systems provide early warnings of potential intrusions in the network. But, they are prone to generate false alarms.

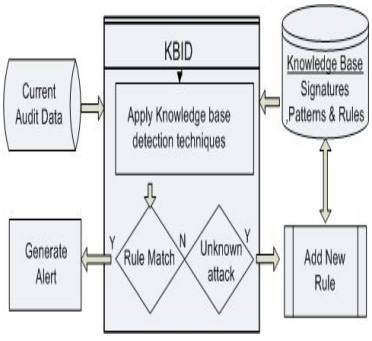



Figure 5:Anomaly-based intrusion detection process

*2) Knowledge-Based Intrusion Detection:* Knowledge based intrusion detection systems contains signatures or patterns of well-known attacks .It looks for these patterns to detect them. The drawbacks of KBID systems are: they can only detect attacks whose signatures or patterns are in the knowledge base.

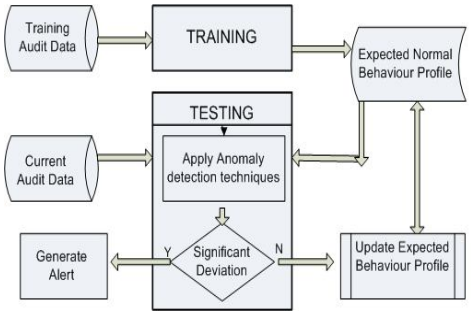



Figure 6: Knowledge-based intrusion detection process

*3) Specification-Based Intrusion Detection:* Specification-based intrusion detection systems (SBIDs) defines specifications as a set of constraints. Then use these specifications to monitor the routing protocol operations or network layer operations to detect attacks in the network.

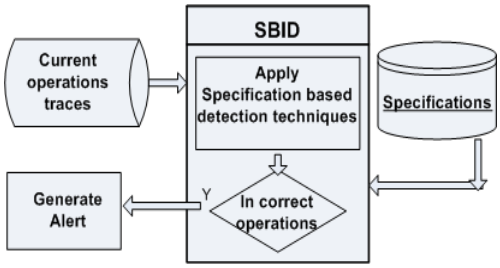
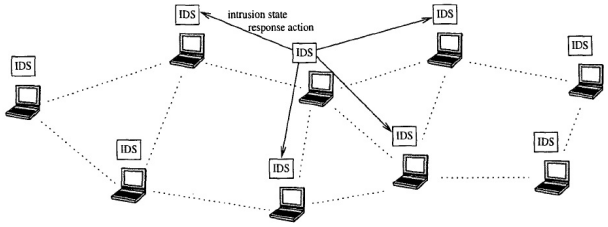



Figure 7:Specification-based intrusion detection process

The first step extracts the specifications, which define the correct operation of (for example) the network or the MAC layer protocol through a set of constraints. The system then monitors the execution of the protocol with respect to the given specification, deviations from the specification being treated as intrusion [17].

*The architecture of the intrusion detection system*:
In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behaviour locally and independently, which are performed by the built-in IDS agent.




*Challenges of Intrusion Detection Systems in MANETs:*

1.It is difficult to capture and gather audit data.
2.It is hard to accurately characterize the normal behaviour of the network.
3.The detection phase has to accommodate the dynamics of MANETs.

*Comparison of point detection algorithms:*

MANETs introduced a new set of routing protocols, which are significantly different from those used in fixed networks. These protocols require nodes to cooperate and act as routers; but it also means that the network's routing infrastructure is not under the control of a single management entity. This has created opportunities for attackers to identify vulnerabilities and find new ways to launch attacks. To overcome the challenges and complexities that IDSs have in MANETs ,the different point detection algorithms either distributed (peer-to-peer) or hierarchical (clustered) are developed.

*Comparison of IDSs for MANETs:*
IDS mechanisms use either ABID, KBID or SBID techniques to identify intrusions, but hybrid techniques, for example GIDP and CRADS deal with network layer attacks. There are mechanisms that deal with multiple attacks by implementing cryptographic techniques, such as ARAN and SEAD. Also ("Intrusion Response" column) that most of the proposals do not consider the response to an attack. The careful selection of the intrusion response can optimise the network's operation .

## III CONCLUSION

The use of MANETs has increased and, consequently, the security issues have become more important. In this paper a survey of significant network layer attacks is reviewed. Also different IDs mechanisms and different point algorithms are highlighted.

## REFERENCES

**[1]** Harish M, Shweta Vincent, ' **A** Survey on Routing Protocols in MANETS', International Journal of Computer Science and Management Research Vol 1 Issue 5 December 2012

**[2]** Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang, and Tarek R. Sheltami, *Member,* **'**EAACK—A Secure Intrusion-Detection System for MANETs.', *IEEE Transactions On Industrial Electronics*, Vol. 60, No. 3, March 2013.

**[3]** Michele Nogueira Lima, Aldri Luiz dos Santos, and Guy Pujolle 'A Survey of Survivability in Mobile Ad Hoc Networks', *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 1, First Quarter 2009

**[4]** Y. Xiao, X. Shen, and D.-Z. Du (Eds.), 'A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks', WIRELESS/MOBILE NETWORK SECURITY 2006 Springer

**[5]** S. Yi and R. Kravets, 'Composite Key Management for Ad Hoc Networks',Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services(MobiQuitous'04), pp. 52-61, 2004.

**[6]** K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, 'A Secure Routing Protocol for Ad Hoc Networks', *Proc. of IEEE International Conference on Network Protocols* (ICNP), pp. 78-87, 2002

**[7]** B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, 'An On-demand Secure Routing Protocol Resilient to Byzantine Failures', *Proceedings of the ACM Workshop on Wireless Security*, pp. 21-30, 2002.

**[8]**Y. Hu, A. Perrig, and D. Johnson, 'Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols'. *Proc. of the ACM Workshop on Wireless Security* (WiSe), pp. 30-40, 2003.

**[9]**Harish M1 , Shweta Vincent 'A Survey on Routing Protocols in MANETS', *Department of Computer Science and Engineering, Karunya University, Coimbatore, India* International Journal of Computer Science and Management Research

**[10]**Karim El Defrawy, Member, IEEE, and Gene Tsudik, Senior Member 'ALARM: Anonymous Location-Aided Routing in Suspicious MANETs', *IEEE Transactions On Mobile Computing*, Vol. 10, No. 9, September 2011

**[11]**Karim El Defrawy, *Member*, and Gene Tsudik 'Privacy-Preserving Location-Based On-Demand Routing in MANETs',*Senior Member, IEEE Journal On Selected Areas In Communications*, Vol. 29, No. 10, December 2011

**[12]**Yi-an Huang and Wenke Lee, 'A Cooperative Intrusion Detection System for Ad Hoc Networks', in *Proceedings of the 1st ACM Workshop on Security of Ad hoc and SensorNetworks*, Fairfax, Virginia, 2003

**[13]**B. Wu, J. Chen, J. Wu, and M. Cardei '*Wireless/Mobile Network Security*', chapter A survey on attacks and countermeasures in mobile ad hoc networks. Springer, 2006.

**[14]**P. E. Ver´ıssimo, N. F. Neves, and M. P. Correia 'Intrusion-Tolerant Architectures: Concepts and Design', *Technical Report DI-FCUL TR-03-5, University of Lisbon, Department of Informatics, University of Lisbon, Portugal*, 2003.

**[15]**Y. Deswarte and D. Powell ' Internet Security: An Intrusion-Tolerance Approach', *Proc. IEEE*, 94(2):432–441, 2006.

**[16]**Adnan Nadeem, *Member, IEEE*, and Michael P. Howarth ' A Survey of MANET Intrusion Detection &Prevention Approaches for Network Layer Attacks', *IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013*

**[17]**P. Uppuluri and R. Sekar, 'Experiences with Specification-Based Intrusion Detection,' Proc. Recent Advances in Intrusion Detection, (RAID),2001.

**[18]**G.F.Cretu, J.Parekh, K.Wang and S.J.Stolfo, 'Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks', *Proc. IEEE Consumer Communication And Networking Conference, 2006*