Intrusion Detection System for Ad hoc Mobile Networks

Muhammad Nawaz Khan
School of Electrical Engineering & Computer Science (SEECS)
National University of Science & Technology (NUST)
Islamabad, Pakistan.

Muhammad Ilyas Khatak, Muhammad Faisal
Department of Computing
Shaheed Zulfikar Ali Bhutto Institute of Science & Technology
Islamabad, Pakistan

ABSTRACT

Proactive security mechanism like authentication, confidentiality and non-repudiation are difficult to implement in MANETs. Some additional security necessities are always desirable like co-operation fairness, location confidentiality, data freshness and absence of traffic diversion. Traditional security mechanism (authentication, encryption) provide abstract level of security but some reactive security mechanism and deep level of inspection is always required. Here local-distributed intrusion detection system for ad hoc networks has proposed. In the proposed distributed-ID, a smart agent in each mobile node analyzes the routing packets and also checks the overall network behavior of MANETs. It works like a Client-Server model using Markov process. The proposed local distributed- IDS shows a balance between false positive and false negative rate.

General Terms

Security, deep level inspection, IDS and mobile ad hoc networks.

Keywords: MANETs, Intrusion Detection System (IDS), security mechanism, proactive, reactive, Markov process, false negative and false positive.

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) is an autonomous system of mobile nodes. Ad hoc network creates from time to time in ad hoc nature and works as wireless network. In MANETs, mobile nodes move from place to place in peer to peer fashion with no central topology. Due to varying nature of MANET, any node may leave or enter the network. The self organizing nature of the ad hoc network comprises the nodes into random and transitory ad hoc topology, this leads to intrinsic weakness of security [1]. Security in an infrastructure-less and ad hoc network is a great challenged. At the same time the resources restraints (limited power, limited communication range, processing capabilities, and limited memory) of the mobile devices in the MANETs leads tradeoff between security requirements and resources utilization [2].

Traditional security mechanism i.e. encryption and authentication, and its successors are used for ensuring security in MANETs. But because of its varying topology and its decentralized management, mobile nodes are compromised in many ways. In fact, these protocols do not scrutinize the received packets and do not examine the overall network performance but works in a traditional proactive manner. Consequently another security level is required which locally analyze the received packets conditions. At this level, it not only inspects receiving packets deeply but also monitors the overall network behavior that what is going on? So if any misbehave action detects, it not only informs the surrounding mobile and static nodes but also take some compulsory action against those intruders. The whole system works in co-operation from base station to mobile nodes. In both variations of ad hoc network, closed-key networks is comparatively more secure than the open ad hoc networks because closed-key networks have pre-define security policy for authentication and encryption. While open ad hoc networks are free for any node to come in and becomes the part of the ad hoc network with arbitrary and temporary topology.

In this paper a cooperative, distributed and local-IDS has proposed. In section-2 of this paper consists on related work in security for ad hoc networks, section-3 discuss MANETs tread model and section-4 have detailed discussion on proposed system. In section-5 the concluding remarks of the paper are included.

2. RELATED WORK

Conventional security mechanisms are insuring by using the concept of key management. But key management becomes difficult in the presence of an active attacker node. A realistic and feasible solution is Certification Authority (CA) [3]. CA has key pair of public and private keys. The public key of the CA is known to everyone. Public key of CA make possible to create digital certificate. Digital certificate have public key for same node sign by its private key [4]. This approach is convincing with a substantial overhead in the network because of dynamically changing topology of MANETs and each times verification of each legitimate node. Another issue is which node becomes CA, if the CA node is being down? Multiple CAs is also recommended but still extra overhead produced in the network by recalculating and verifying nodes. Another solution is distributed CAs. But experiments show that distributed CAs also did not solve the network overhead problem [5]. In all these schemes CA is responsible for identification of each node by checking certificate validity. It prevents spoofing and other malicious activities and identifies legitimate nodes. But certificate verification requires a strong management system between CAs and surrounding nodes. This creates extra packets roaming all times in ad hoc network for creation and verification of certificate. All this extra traffic produces overhead in such resource constraint network like MANETs. Symmetric key encryption is also used for authentication and authorization process for mobile nodes within the MANETs. But network layer related issues and concerns are also encounter when such approach is used for ad hoc networks [6]. Another approach is localized certification based on public key infrastructure (PKI). In this scheme, CAs and nodes updates its revocation list by using shared a secret [7]. But PKI also based on same infrastructure with more overhead and latency in the ad hoc network. Secure Routing Protocol (SRP) is another solution. SRP discovers secure and correct routs from time to time so that compromised and re-played route are find out and must be rejected. Security associations are exits between ends nodes that no intermediate nodes are take participate in path discovery. The unique identifier number and authentication codes are used for correct rout discovery [8]. For fast and quick analysis in ad hoc networks an IDS based Systems Analysis and Integration is

proposed. The proposed mobile agent-based IDS create local character repository, updating with time. To reducing network overhead only concerned node apply agent operation to avoid broad casting and blocking the network and therefore the overall network works in normal fashion [13]. Considering the special architecture of MANETs, novel mobile agent based IDS architecture has been proposed. In this proposed architecture each node implements basic IDS functions while ranger agents roam the network executing more advanced IDS functions. Additional functionality provided by these mobile agents moving around the network when needed [14]. In [15] node-based intrusion detection system (IDS) for wireless ad hoc networks has been proposed. In the proposed work information from MAC layer and network layer are correlates for normal behavior of the mobile node. They also suggest rule-based data mining technique for anomaly detection. Decision module minimize false positive rate while Bayesian network is added to evaluate multiple attacks. Evaluation results shows effectiveness of the proposed work. In [16], Ad-hoc On-Demand Distance Vector (AODV) routing protocol is used for quick adaptation to dynamic links, low processing and memory overhead and also for low network utilization. The security structure has built on key handling. The one way key chain is useful because the mobile nodes first authentic themselves to the surrounding node before communication. The main focus of the proposed is low overhead. In [17], based on Suburban Ad-hoc Network (SAHN) an intrusion detection system been proposed known as SAHN-IDS. SAHN-IDS useful for multi hop ad hoc network, where it detects misbehavior node by getting unfair share of transmission channel. It also detects anomalies in packet forwarding in effective and unique. The simulation results show the efficiency of the proposed scheme. In [18], a novel intrusion detection and response system has been proposed known as Routeguard. It successfully detects malicious mobile node and hence protect the network. Routeguard mainly work on the concept of monitoring and node cooperation. Simulations show the effective of the scheme. In [19], a "Cross Layer Based Intrusion Detection System"(CIDS) has been proposed for ad hoc networks. It detects intruders by analyzing the pattern of trace files. It communicates data securely from source to destination which increase network efficiency. In [9], co-operative and distributed IDS for ad hoc networks have proposed which works on statistical anomaly based detection.

Many other IDS for ad hoc network are proposed, but the principle is the same that all IDSs are design to protect the MANETs from outsider and insider attacks. The proposed local distributed-IDS are different in working mechanism from previous approaches. It is very effective in those situations where malicious codes play an important role in inside and outside network attacks.

Due to unique characteristics of MANETs, all the above approaches are rarely implemented in practical scenarios. The researchers want a feasible solution that not only analyze network performance but also deeply inspect the incoming packets to ad hoc network.

3. THREAD MODEL

The ad hoc wireless connectivity and dynamically changing topology with limited resources makes the MANETs more vulnerable to active and passive attacks. Most of the attacks are man in middle or denial of services (DoS) in nature. In DoS attacks, the goal of the attacker is to obtained information or cryptographic keys to damage or replace a mobile node. In DoS actually utilize system resources and cause it malfunction [16]. The DOS attack in MANETs launched by the laptop node in the network. Laptop node has more resources compared to other mobile nodes in the network. DoS attack can activate at any layer in MANETs. At physical layer, DoS launched by continuously transmitting the signals which interferes the radio frequencies of the ad hoc network. This continuous retransmitting busy or jams the ad hoc network and effected for desire functionality of the network. At data link layer, DoS attack is launched by violating communication protocol. These communication protocols continually retransmit massages to generate collision. This retransmission effects node functionality by utilizing the energy of the mobile node. At network layer, the DOS attack affects all routing protocols in different ways [10]. One sophisticated routing protocol attack is routing disruption attack. In which the attacker node generate randomly constructed routing control packets and distribute them into the network. This bogus information prevents the source node from established the accurate path for routing [19]. DoS attack is more sophisticated in MANETs. There are too many types of DoS attack for MANETs. One dedicated DOS attacks in MANETs is Black hole router attack. In which the malicious node gets information from the surrounding nodes by claiming to be the path node and do not forward these information to the base station. Another dedicated DoS attack for MANETs is HELLO flood attack or resource exhaustion attack. In which the malicious mobile or static node broad cast or uni-cast HELLO massages again and again to the target nodes. Which utilize the resources, most of the time battery of the target node [12]. Another DoS attack in MANETs is routing loop. In which a loop is created in routing path, which circulate the data again and again and therefore did not reached to base station. MANETs also suffers from various types of Man In Middle (MIM) attacks. MIM attacks are launched easily due to the wireless nature of the ad hoc network. There are many types of MIM attacks been discovered in MANETs. Sybil Attack is one them, in which a single malicious node masquerading with multiple identities. Sybil attack is more serious impact on fault-tolerant schemes of the ad hoc network [10]. While in replication attacks, target node is capture, analyze, reprogram it and replicate it. These replicas are now inserted onto network at different location for various activities [10]. Attacking network is another one. In which malicious node partitions the connected network into small and sub networks. These sub network created in such way that they cannot communicated although they are connected [11]. Insider malicious and selfish nodes in network can also corrupt or miss guide the data. Although the ad hoc networks have no central monitoring system and no central aggregation point. But today ad hoc networks are beyond this restriction. They have not only a base station but central management information system. Many variation of ad hoc network with central base station exists. As the base stations plays an important role such networks. All decisions about network management are decide at base station. Therefore certain dedicated attacks are launched to compromise base station. And if any way base station has been compromised it means the entire network compromised. Hence it has been trying to protect base station from inside and outside attacks.

4. PROPOSED SYSTEM

There are numerous Intrusion Detection Systems (IDS) for ad hoc network have been proposed. Some of them have significant for certain scenarios while some of them are used with alliance of routing protocols. Here we propose distributive local IDS for ad hoc mobile networks. The local-IDS may be used for low energy nodes like sensor nodes. Sensor nodes have limited resources, design for special purpose. Proposed local-IDS can also used for

more power full mobile nodes, having more resources. It is distributive because each node in the network analyze the data individually and independently by smart agents and therefore each node have work as an IDS agent distributed into the whole network. It is local because each node check data/network behavior locally and it is co-operative because it informs other nodes as well as base station to takes some action collectively against such malicious activity. The data received by the mobile or static nodes in the ad hoc network, first deeply inspects for malevolent code and also monitors all network performance by analyzing network behavior with regular intervals.

In proposed scheme, first the data is collected and analyzed for intruders and then takes an appropriate action on analyzed data. Each node has their own local-IDS agent for checking the received data. These agents have some previous signature or pre-define profile. When data is entered into these agents, the node first analyze the receiving data by comparing it for normal and abnormal activities with the threshold value of the pre-define profile. If certain activity detecting as malicious or find some signature for harmful code. It informs the base station or cluster head for further analysis and for appropriate action. This node also informs the surrounding nodes, to aware of such falsified or malicious data. The local-IDS agent should be program in such way that it must detect normal and abnormal activities. The smart agent works on Markov process, each node must updates its profiles/signature according to the base station commands. When base station receives the data that having complaint massages from the node, the base station first analyze the same abnormal behavior/malicious data. And base station informs rest of the cluster heads in that particular area and also informs other base station for this abnormal activity/malicious data. The base station, now watch the overall network behavior and also check the updates coming from other cluster heads as well as from other base stations. All these activities help on the base station to confirm the performance of the network. The base station sends updates to other nodes using Markov process. The last node in the hierarchy receives the difference of all of the nodes from base station to the last node. The net difference between two profiles/signatures is the signature updates. The whole process needs a high level of co-operation between base station and mobile nodes which make the proposed IDS more intelligent and useful.

5. SYSTEM MODEL

The local-IDS with each mobile or static node consist of six parts. The main parts of the Local-IDS agent are shown in figure.1. First data is collected by collection and control module. It is "collector" because it collects data from other nodes; it is "controller" in a sense that it controls all the activities of the local IDS agent. Collected data then moved to analyzer module for analysis. The analyzer actually decided the working principle. This part of the system depends upon the system design it works on protocol analysis (algorithm), pre-define profile or pre-define signature. The analyzer module is actually the main place where the base station preserve the pre-define signature or profile for each node. The updates from the base station to local-IDS agents based node, are come through Markov process. If analyzer module is tightly design then it increases the false positive rate which collected erroneous as well as correct data. But the analyzer module must decreases the false negative because in that case erroneous data is also marked as correct data. So analyzer module is design in such way that they show the balance between false positive and false negative. After analyzer, the data is either pass to the safe module or emergency module. Data in the safe module show normal data having no abnormal code. Safe module sends data to global response module (GRM) for sending base station on normal basis. The safe module also play important role for those data which already mark as malevolent by leaf node in sequence. The emergency module is also known as Local Response Module (LRM). If data is passing to local response module, it means the analyzer find something wrong in the data/abnormal system behavior, so LRM send an alarm massage to surrounding nodes. The data then pass into priority module, where priorities are assign to those packets and sends it to GRM. The GRM send it to the base station for further analysis. The base station then further investigate these packets and send massages to other base station and cluster heads as well as to the co-operative nodes. The controller of the IDS at each node receives those massages and responds consequently. The base station checks the overall data flow, over all behavior of the network and receive messages from other base station as well. The base station then follow a procedure how to undertake the intruders and how mange the overall network.

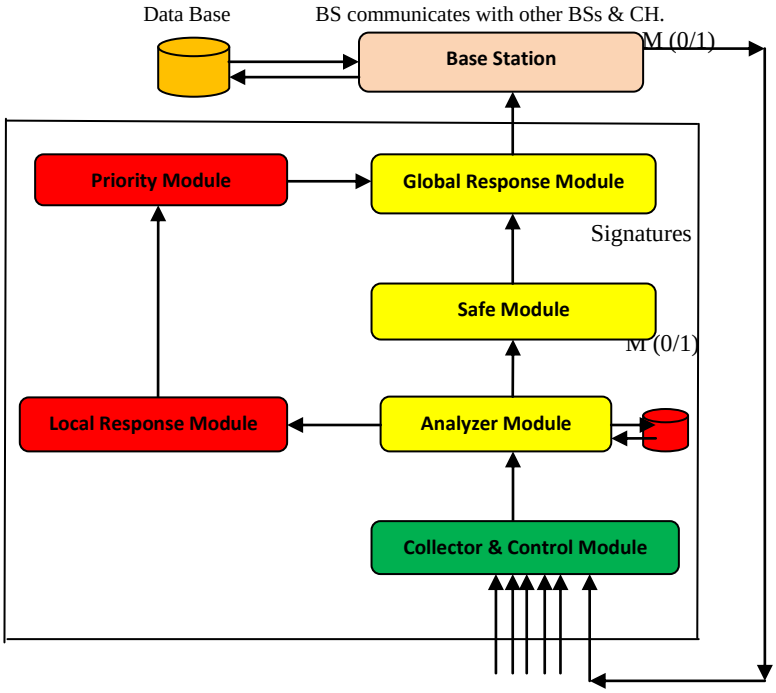


Fig.1 System Model of Local-IDS node.

The distributed local-IDS is actually the smart agents based IDS. In which data is collected locally by these smart agents and if something find anomalous by comparing the profiles or signature with predefine profile or signature. It sends those data on priority bases to base station and also informs the surrounding nodes about those malicious data. The base station is, in fact, monitoring the overall network performance by analyzing the behavior of the nodes. For example if network consist on five hundred nodes and two hundred nodes are suddenly down or some existing paths are suddenly change, then the base station look for those abnormal behavior and respond like a typical intrusion prevention system by saving further network damage. The base station is actually tells the controller of the agents, what to do? How to do? And when to do? If the base station finds some malicious activity continuously acting

on surrounding nodes (like in DOS attack), the base station sends instructions the controller that do not collect data until next command is received for recollection. The base station also tells the nodes that this type data are not send to base station comparing to some signature. For re-collection, the base station tells the nodes to collect the data by sending a massage having one for collection and zero for dropping the data. The base station sends updated signature to the agents for comparison by using Markov process. In real scenarios the base station may be far away from sensing node. So the data is send through other nodes, in that case the data is not check by each node if some priority is assign to it. The safe module plays an important role in that case. The priority assign values is send first because it important. An algorithm must maintain how to assign priorities and how to send such packets before any data send. In fig.2, the system flow chart shows the overall structure of Local-IDS related to base station.

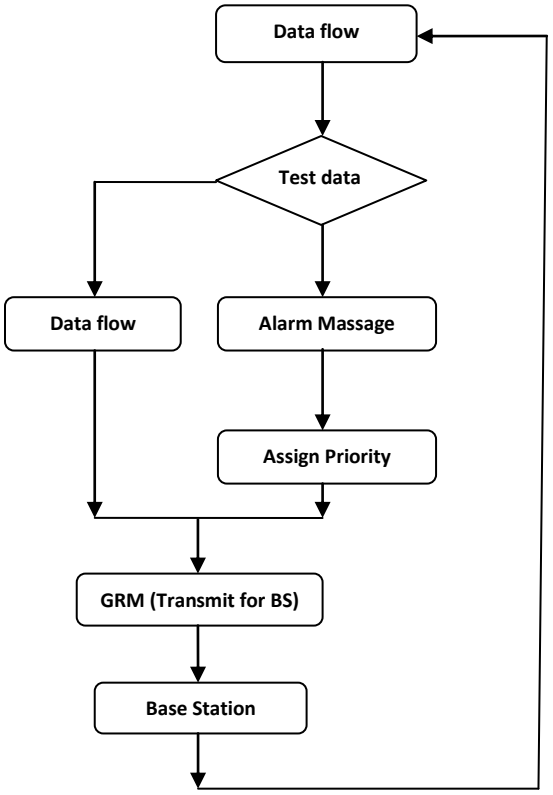


Fig.2 System Flow chart

6. SIMULATIONS AND FUTURE WORK

Consider a mobile ad hoc network having many nodes each them having an intrusion detection system (smart agents). Each of them is capable of checking the incoming packets to the MANETs. Consider the following simulation parameters. A network consisting of MANETs nodes having communication range from 150 t0 200 meters, covering an area of 500 by 500 square meters. These MANETs nodes can move any direction, the base station also randomly moves. Maximum speed of each node 5 meter per second but a node can also have less velocity. Transmission capacity of each node is 1.5 Mbps, with initial set count of 20. Total flows in the network when initially test is 10. Testing execution time is 50 seconds, and average transmission flow of the network is 2 packets per second.

Topology shape	500 meter *500 meter
Radio Range of each node	150-200 meters
Node moments	Random
Base Station Moment	Random
Topological Model	Multi hop planner/hierarchical
Maximum speed of a node	5 meters/second
Transmission Capacity	1.5 Mbps
Set Node count	20
Total flows	10-15
Average transmission per flow	2 packets per second
Testing execution time	50 seconds

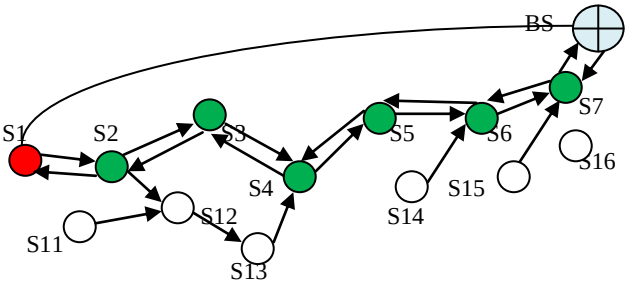
Tables.1 Simulation Parameters

Each node in the topology updates its pre-define/signature by using the Markov process. For example

$$p(w,x)Up(x,y)Up(y,z) = \sum(BS)$$

$$\sum(BS) = p(S1,S2)Up(s2,s3)Up(s3,s4) \ldots . Up(sn-1,sn)$$

Above equation shows the Markov process for given ad hoc topology. The current threshold of the leaf node (red color) is updated from deference of all the visiting nodes in the way to the base station. The current state of a node depends upon the previous state of the node or the threshold of the above node in the hierarchy. The difference of the nodes (S1 & S2) are compared automatically to the difference of (S2 & S3), in the same way all the path difference from base station to leaf node is reached. The leaf node signature is actually different from the previous node signature but very matching to surrounding nodes.



So S1 gets updates from S2 and S2 gets updates from S3 and so on up to S7 which is near to the base station, it gets updates from base station. The base station also sends messages in the same way as receive messages. When analyzer node detects data as malicious, it assigns a priority to those packets. For example S1 detected such packets, then other nodes S2, S3, S4, S5, S6, S7, do not check it, it just passed those packets to base station as quick as possible. The safe module plays an important role in forwarding of prioritized messages. The base station further analyzes the data and sends a message to the cluster heads. As denial of service (DOS) attack is

so common in MANETs. The local-IDS prevents such attacks by analyzing packets in term pre-define profiles/signature and also monitoring the overall performance of the network at base station.

7. CONCLUSION

Instead of proactive security mechanism some reactive security mechanism are required for MANETs, because the ad hoc nature of the network. In this paper we proposed Local-IDS, work locally in co-operative manner, locally analyzed the data/network behavior, if something is going in wrong direction, it not only inform local nodes but also inform the base station for further analysis. The distributed nature of local-IDS not only secures the ad hoc networks but also helps in that environment where no central management is ensuring like MANETs.

8. REFERENCES

[1] Poly Sen, Nabendu Chaki, Rituparna Chaki "HIDS: Honesty-rate Based Collaborative Intrusion Detection System for Mobile Ad-Hoc Networks".

[2] "Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness." By Sonja Buchegger, Jean-Yves Le Boudec .

[3] M. Gasser, A. Goldstein, C. Kaufman, B. Lampson, "The Digital Distributed Systems Security Architecture," 12th National Computer Security Conference.

[4] Wensheng Zhang, R. Rao, Guohong Cao, GeorgeKesidis "SECURE ROUTING IN ADHOC NETWORKS AND A RELATED INTRUSION DETECTION PROBLEM".

[5] L. Zhouand Z. Haas, "Securing Ad Hoc Networks," IEEE Net-work

[6] Frank Stajano and Ross Anderson. "The Resurrecting Duckling." Lecture Notes in Computer Science, Springer-Verlag, 1999.

[7] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, Lixia Zhang. "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks." In International Conference on Network Protocols (ICNP), pages 251–260, 2001

[8] Panagiotis Papadimitratos and Zygmunt J. Haas. "Secure Routing for Mobile Ad Hoc Networks" In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference. (CNDS 2002), San Antonio, TX, January 2002

[9] Yongguang Zhang and Wenke Le " Intrusion Detection in Wireless Ad-Hoc Networks" In Proceedings of MOBICOM 2000

[10] Michael Healy, Thomas Newe, Elfed Lewis "Security for Wireless Sensor Networks: A Review" Optical Fibre Sensors Research Centre, Department of Electronic and Computer Engineering, University of Limerick, Limerick, Ireland.(2009).

[11] Yi-an Huang, Wenke Lee. " A Cooperative Intrusion Detection System for Ad Hoc Networks ".

[12] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks-The routing problem".

[13] Hua Zhou, Junlin Li, Na Zhao, Fei Dai and Rong Jiang. "An Intrusion Detection System Model for Ad Hoc Networks Based on the Adjacent Agent". International Conference on Multi Media and Information Technology 2008.

[14] Yinghua Guo and Steven Gordon "Ranger, a Novel Intrusion Detection System Architecture for Mobile Ad Hoc Networks".

[15] Yu Liu, Yang Li, Hong Man. "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks". Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) 2005 .

[16] Rakesh Shrestha, Jong-Yeop Sung, Sang-Duck Lee, Pyung Sik-Yun, Dong-You Choi and Seung-Jo Han. "A Secure Intrusion Detection System with Authentication in Mobile Ad hoc Network". Pacific-Asia Conference on Circuits,Communications and System. 2009

[17] Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp. "An Intrusion Detection System for Suburban Ad hoc Networks"

[18] S.Bose and A.Kannan. "Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks". IEEE-International Conference on Signal processing, Communications and Networking, Jan 4-6, 2008

[19] O. Kachirski and R. Guha, Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks, Knowledge, July 10–12, 2002.