THE EVOLUTION OF IDS SOLUTIONS IN WIRELESS AD-HOC NETWORKS TO WIRELESS MESH NETWORKS

Novarun Deb[1], Manali Chakraborty[2], Nabendu Chaki[3]

Department of Computer Science & Engineering, University of Calcutta, India

92 APC Road, Kolkata 700009, India

[1]novarun.db@gmail.com, [2]manali4mkolkata@gmail.com, [3]nabendu@ieee.org

ABSTRACT

The domain of wireless networks is inherently vulnerable to attacks due to the unreliable wireless medium. Such networks can be secured from intrusions using either prevention or detection schemes. This paper focuses its study on intrusion detection rather than prevention of attacks. As attackers keep on improvising too, an active prevention method alone cannot provide total security to the system. Here in lies the importance of intrusion detection systems (IDS) that are solely designed to detect intrusions in real time. Wireless networks are broadly classified into Wireless Ad-hoc Networks (WAHNs), Mobile Ad-hoc Networks (MANETs), Wireless Sensor Networks (WSNs) and the most recent Wireless Mesh Networks (WMNs). Several IDS solutions have been proposed for these networks. This paper is an extension to a survey of IDS solutions for MANETs and WMNs published earlier in the sense that the present survey offers a comparative insight of recent IDS solutions for all the sub domains of wireless networks.

KEYWORDS

Intrusion, Intrusion detection systems, trust, wireless ad-hoc networks, MANET, wireless mesh network, wireless sensor network.

1. INTRODUCTION

An intrusion may be defined as any action that attempt to compromise the integrity, confidentiality or availability of a resource or that goes against the security goals of a resource. This can be something as severe as stealing confidential data or misusing the email system for spam. External intrusion attempts are targeted to cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely. The internal intrusions could be a lot more damaging since malicious insider already belongs to the network as an authorized party. Since prevention of intrusions is not always possible, supportive intrusion detection techniques are required. Intrusion detection systems (IDSs) are not to prevent or deter attacks. Instead, the purpose is to alert the users about possible attacks, ideally in time to stop the attack or mitigate the damage [1].

Detecting Intrusion is difficult, particularly in the wireless domain. IDS often attempts to differentiate abnormal activities from the normal ones. Unfortunately, normal activities can be varied, and an attack may have resemblance to normal activities. Also, consistency of data in the

DOI : 10.5121/ijnsa.2011.3603

time domain can detect unusual behavior but unusual behavior is not necessarily malicious. An IDS reaches perfection if it accurately detects majority of attacks and hardly makes any false or phantom detection. One basic assumption while designing any IDS should be that the attacker is intelligent and that the attacker has no shortage of resources.

An IDS essentially consists of three functions. First, the IDS must monitor some event and maintain the history of data related to that event. Second, the IDS must be equipped with an analysis engine that processes the collected data. It detects unusual or malicious signs in the data by measuring the consistency of data in the time domain. Currently there are two basic approaches to analysis: misuse detection and anomaly-based detection. Third, the IDS must generate a response, which is typically an alert to system administrators. It is up to the system administrator, how he wants to scrutinize the system after receiving an alert.

1.1. The Evolution of networks and their Security

After an era of providing solutions in the domain of infrastructure based wired networks, several commercial applications cropped up which required providing services to clients on the go. This basic need led to the development of Wireless Ad – Hoc Networks. Once protocols and standards were developed for WAHNs, the need for security became but obvious.

To protect networks from adversaries, we investigated security issues in Ad Hoc Networks (AHN), based on our knowledge in securing wired networks. AHNs were prone to the same types of attacks as wired networks. Furthermore, the openness of wireless communication media and node mobility made AHNs more vulnerable than traditional networks to attacks. Anyone with a scanner could monitor traffic from the comfort of his or her home or the ease of a street corner. With a powerful jamming machine, an attacker could reduce the channel availability or even shut down communication channels [43].

Wired networks were built over time. They reflected security policies of organizations. Trust between entities, an essential element of a security policy, was also built over time. System administrators supported network operations such as implementing security policies. In comparison, AHNs were built quickly and as needed. Trust and policies were put together in a hurry. Mobility and some physical features (e.g., small size) of nodes made them more easily compromised and lost than those in wired networks.

Different AHNs have different initial contexts and requirements for security depending on applications. However, they all share one characteristic: no fixed infrastructure. The lack of infrastructure support led to the absence of dedicated machines providing naming and routing service. Every node in an AHN became a router. Thus network operations had higher dependence on individual nodes than in wired networks. The mobility of nodes brought constant change in network topology and membership, making it impractical to provide traditional, centralized services [43, 44].

The unreliability of wireless links between nodes, constantly changing topology owing to the movement of nodes in and out of the network, and lack of incorporation of security features in statically configured wireless routing protocols not meant for ad hoc environments all led to increased vulnerability and exposure to attacks. Security in wireless ad hoc networks was particularly difficult to achieve, notably because of the vulnerability of the links, the limited physical protection of each of the nodes, the sporadic nature of connectivity, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. This, in effect, underscored the need for intrusion detection, prevention, and related countermeasures.

The absence of infrastructure and the consequent absence of authorization facilities impeded the usual practice of establishing a line of defence, distinguishing nodes as trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials, and the ability of nodes to validate them. In the case of wireless ad hoc networks, there might have been no ground for an a priori classification, since all nodes were required to cooperate in supporting the network operation, while no prior security association could be assumed for all the network nodes [45].

Mobile ad hoc networks were vulnerable to a wide range of active and passive attacks that could be launched relatively easily, since all communications take place over the wireless medium. In particular, wireless communication facilitates eavesdropping, especially because continuous monitoring of the shared medium, referred to as promiscuous mode, was required by many MANET protocols. Impersonation was another attack that became more feasible in the wireless environment. Physical access to the network was gained simply by transmitting with adequate power to reach one or more nodes in proximity, which may have no means to distinguish the transmission of an adversary from that of a legitimate source. Finally, wireless transmissions could be intercepted, and an adversary with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms could obstruct its neighbours from gaining access to the wireless medium.

In addition, freely roaming nodes join and leave MANET sub domains independently, possibly frequently, and without notice, making it difficult in most cases to have a clear picture of the ad hoc network membership. In other words, there may be no ground for an a priori classification of a subset of nodes as trusted to support the network functionality. Trust may only be developed over time, while trust relationships among nodes may also change, when, for example, nodes in an ad hoc network dynamically become affiliated with administrative domains. This was in contrast to other mobile networking paradigms, such as Mobile IP or cellular telephony, where nodes continue to belong to their administrative domain in spite of mobility. Consequently, security solutions with static configuration would not suffice, and the assumption that all nodes can be bootstrapped with the credentials of all other nodes would be unrealistic for a wide range of MANET instances [45, 46].

The absence of a central entity made the detection of attacks a very difficult problem, since highly dynamic large networks cannot be easily monitored. Benign failures, such as transmission impairments, path breakages, and dropped packets, were naturally a fairly common occurrence in mobile ad hoc networks, and, consequently, malicious failures would be more difficult to distinguish. This will be especially true for adversaries that vary their attack pattern and misbehave intermittently against a set of their peers that also changes over time. As a result, short-lived observations would not allow detection of adversaries.

Moreover, abnormal situations occurred frequently because nodes behaved in a selfish manner and did not always assist the network functionality. It was noteworthy that such behaviour may not be malicious, but only necessary when, for example, a node shuts its transceiver down in order to preserve its battery [46].

Thus, from obvious reasoning, it can be anticipated that providing an infrastructure to Ad-Hoc Networks had become the need of the hour. The next advancement in networking environments was Sensor Networks.

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges [47]. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of

data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. The unreliable communication channel and unattended operation make the security defences even harder. Indeed, as pointed out in [30], wireless sensors often have the processing characteristics of machines that are decades old (or longer), and the industrial trend is to reduce the cost of wireless sensors while maintaining similar computing power.

With that in mind, many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. All aspects of the wireless sensor network are being examined including secure and efficient routing [46, 48, 49, 50], data aggregation [51, 52], group formation [53], and so on.

In addition to those traditional security issues, we observe that many general-purpose sensor network techniques (particularly the early research) assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security [54, 55]. In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks.

Thus, although mobility of nodes was removed and a certain infrastructure was established for Sensor Networks, yet WAHNs remained vulnerable to security threats. Researchers realized that mobility is a feature which cannot be compromised with as it provides tremendous flexibility to end users. Yet, retaining an infrastructure would definitely be helpful. All these underlying observations led to the conclusion that a different type of network must be designed which incorporates both the mobility of clients and a basic infrastructure. This was the inception of Wireless Mesh Networks.

Wireless Mesh Networks (WMNs) are an extension of existing Wireless Ad hoc Networks to eliminate the limitations of the current network structures and also improve the performance of the overall network. It provides the advantages of both infrastructure based static network and infrastructure less mobile network. A WMN usually consist of mesh routers and mesh clients. Mesh clients are generally mobile and they are responsible for the automatic establishment and dynamic up gradation of mesh topology among the nodes and also act as a router for the other nodes in the network. Thus make the network dynamic, scalable and robust. On the other hand the mesh routers are generally static and provide an infrastructure based backbone for the WMNs. Mesh routers can integrate different existing wireless networks with the help of gateway and bridges. They also provide network access for both mesh and conventional clients [26].

1.2. Organization of the paper

In this paper, we have studied most recent works for IDS for all types of wireless ad-hoc networks. This is an extension of a similar survey in [56] that covers only MANETs and mesh networks. Section 2 of the paper analyzes IDS solutions for Wireless Ad-hoc Networks. In section 3 of this paper, we have reported and analyzed seven different IDS approaches for MANET out of which four has been published in last 4 years. In section 4, six different IDS solutions have been reported for Wireless Sensor Networks. In section 5, 100% of the six reported IDS approaches on wireless mesh networks have been proposed in last 2 years. Each of

the sections 2, 3, 4, and 5 ends with separate tables highlighting the basic features and limitations of the existing IDS solutions.

Survey papers like this one often include simulation results to compare different approaches. However, here the authors have carefully avoided simulation for performance evaluation for a couple of reasons. Firstly, different approaches for intrusion detection assume different configurations in the network. Even the underlying routing protocols are not the same. Some of the approaches claim to be compatible with multiple existing routing protocols. However, there would be significant impact in the simulation results for such variance. This in turn would spoil the entire purpose of the simulation. Besides, the paper covers a total of 25 IDS solutions, most of which have been published very recently. Usually simulation based graphs are good for comparing a small number of alternate solutions. Thus, instead of simulations, the authors have followed a careful analytic approach to compare the works referred.

2. IDS FOR WIRELESS AD-HOC NETWORKS

The basic idea behind ad-hoc networks is that the formation of networks is on the fly. The result is an on-demand network, in contrast with the conventional wired networks where their establishment requires fixed infrastructure. Thus all the usual rules about fixed topologies, fixed and known neighbors, fixed relationship between IP address and more are suddenly tossed out the window. Once protocols and standards were developed for ad-hoc networks, the need for security became but obvious. The openness of wireless communication media and node mobility made ad-hoc networks more vulnerable than traditional networks to attacks.

The absence of infrastructure and the consequent absence of authorization facilities impeded the usual practice of establishing a line of defense, distinguishing nodes as trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials, and the ability of nodes to validate them. In the case of wireless ad hoc networks, there might have been no ground for an a priori classification, since all nodes were required to cooperate in supporting the network operation, while no prior security association could be assumed for all the network nodes [18].

Ad-hoc networks are prone to the same types of attacks as wired networks. In addition, the openness of wireless communication media and node mobility makes ad-hoc networks more vulnerable than wired networks. Any intruder with a scanner could monitor traffic from the comfort of his home. With a powerful jamming device, an attacker could reduce the channel availability or even shut down communication channels [19, 20]. Some of the protocols that were developed for WAHNs are explained below. A comparative study is provided at the end of this section.

One of the first intrusion detection algorithm was called Watchdog and Path raters. [21]. In this method, each node runs a standalone IDS that detects attacks independently over DSR protocol. This algorithm uses a stand-alone architecture. A unique characteristic of this method is that it detects malicious nodes but does not report about them to other nodes. The watchdog scheme is limited to source routing because the watchdog needs knowledge of the proper route for each packet. It is also vulnerable to interference by a malicious node falsely reporting other nodes as misbehaving. Multiple misbehaving nodes could collectively interfere with the watchdog process. Lastly, a misbehaving node could escape detection by dropping packets just below the threshold level. The two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and path rater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

The next IDS [22] was based on Static Stationary Database (SSD) and its basic methodology was Mobile agent based Anomaly, Misuse & Hybrid Detection with independent decision-making. SSD are stored in areas having high physical security; yet there is risk of attack. SSDs limit the amount of communication that must take place between IDS agents in the mobile ad hoc network .The use of the SSD to mine new anomaly rules is beneficial to the IDS because the SSD will be a fixed, fast machine that is capable of mining rules much faster than on slower, mobile nodes. The SSD is also capable of having much more storage capacity to store an abundance of audit data collected from the nodes and the newest misuse signatures specified by the system administrator. But, if a SSD is used, nodes will have to be attached to the non-mobile database periodically to stay up-to-date with the latest intrusion information. Also, since the SSD must be a trusted source, it cannot be taken onsite without significant risk.

In the year 2002 Local Intrusion Detection System (LIDS) [23] was proposed. It employed several data collecting agents like- LIDS agent, mobile agent and MIB agent. The basic methodology was Mobile Agent based Distributed Anomaly detection with independent decision making. The cost of local information collection is negligible. Different LIDS might be run on different operating systems or use data from different activities such as system, application, or network activities; therefore, the format of this raw data might be different, which makes it hard for LIDS to analyze. However, such difficulties can be solved by using SNMP (Simple Network Management Protocol) data located in MIBs (Management Information Base) as an audit data source. To obtain additional information from other nodes, the authors proposed mobile agents to be used to transport SNMP requests to other nodes. The idea differs from traditional SNMP in that the traditional approach transfers data to the requesting node for computation while this approach brings the code to the data on the requested node. This is motivated by the unreliability of UDP messages used in SNMP. As a result, the amount of exchanged data is tremendously reduced.

Another multi-sensor intrusion detection system based on mobile agent technology was proposed in 2002 [24]. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. In addition, the hierarchical structure of agents is also developed in this intrusion detection system. The network is logically divided into clusters with a single cluster-head for each cluster. The network monitoring agent (with network monitoring sensor) in the cluster-head will monitor the packets within the cluster and only packets whose originators are in the same cluster are captured and investigated. Then the decision agents performs the decision making based on the collective information, thus, other nodes have no influence on its decision. This way, spoofing attacks and false accusations can be prevented; however, the amount of information obtained by a decision-making node about each node participating in the network is limited. The rationale is that a node is located in close proximity (within two hops) to the packet-monitoring node, and rapid movement may position the node within a communication range of that packet-monitoring node. Such a decision scheme avoids denial of service (DOS) attacks.

For the first time in the year 2003, a hierarchical architecture for Intrusion Detection systems - Real time Intrusion Detection for Ad hoc Network (RIDAN) [25] was proposed. The basic working principle was misuse detection and specification based detection. It utilizes TFSM to detect real time attacks. Though it is not a complete secure system, it has less error compared to other researches. RIDAN manages to keep the delivery ratio higher, at around 60%, having a significant improvement on other protocols. Some standard protocols, like AODV performs better with RIDAN. RIDAN was tested in terms of detection accuracy and the percentages of successful detection for the three attacks are the following:
Sequence number attack detection accuracy: 81.2%,

Dropping routing packets attack detection accuracy: 71.5%,
Resource consumption attack detection accuracy: 74.8%.
The detection accuracy of RIDAN in all the three attacks can be considered high compared to the results of other similar projects [26, 27, and 28]. However, RIDAN is not a complete security solution for ad hoc networks. It is not able to detect attacks that involve impersonation since we do not employ cryptographic mechanisms for address authentication.

Table 1. Summary on Comparison for Different IDS for Wireless Ad-hoc Networks

IDS Reference	Under-lying Routing Protocol	Architecture	Types of attacks addressed	Comments
Mitigating routing misbehaviour in mobile ad hoc networks. (2000).	DSR	Stand alone IDS.	Malicious nodes.	• Mitigate the effects of compromised nodes Improve throughput. • Detect misbehave nodes at the forwarding level. • Detect Malicious Nodes but does not report to other nodes. • The main problem with this approach is its vulnerability to blackmail attacks.
An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks. (2001).	Not identified	Mobile IDS agent and Stationary secure data	Malicious nodes	• Mobile agents do intrusion detection by using: ADM, MDM • The use of SSD limits communication between IDS Agents • SSD is stored in high physical security area. However, it indeed remains a concern to secure the SSD. • Periodically up to date with non-mobile data-base.
Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. (2002)	Not identified	Distributed and Collaborative	Malicious nodes.	• Use SNMP data located in MIB to process data • Transmit SNMP requests to remote hosts to overcome the unreliability of UDP, by using mobile agent. • Cost of local information collection is negligible by running SNMP agent on each node
Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks. (2002)	Not identified	Distributed.	Spoofing attacks	• Multiple sensors used to implement a bandwidth conscious scheme • Distributed IDS make better network performance
Real-time Intrusion Detection for Ad hoc Networks. (2005)	AODV	Hierarchical	Packet Dropping, Resource consumption attacks	• Utilize TFSM to detect real time attacks • Minimize the effectiveness of attacks • Has less error compare with other researches • Is not complete secure system

3. IDS FOR MOBILE AD-HOC NETWORKS

A Mobile Ad hoc Network (MANET) can be defined as a collection of mobile nodes that are geographically distributed and communicate with one another over a wireless medium. Ideally, in a MANET, each node is assumed to be a friendly node and participates willingly in relaying messages to their ultimate destinations. A mobile ad hoc network is built on ad-hoc demand and consists of some wireless nodes moving within a geographically distributed area. These nodes can join or leave the network at any time. MANET does not use fixed infrastructure and does not have a centralized administration. The nodes communicate on a peer-to-peer basis. The networks are built on the basis of mutual cooperation and trust. This leads to an inherent weakness of security.

Security in mobile wireless ad hoc networks was particularly difficult to achieve, notably because of the vulnerability of the links, the limited physical protection of each of the nodes, the sporadic nature of connectivity, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point [11]. This, in effect, underscored the need for intrusion detection, prevention, and related countermeasures. Like any other research area, one needs to do a systematic re-search of the existing works in the area of intrusion detection too. In a very recent paper [4], a number of IDS methods have been described for MANET. Although the compilation is good, no serious attempt has been initiated to identify the gaps in the works cited. Survey papers on IDSs for Wireless Mesh Networks are very few in numbers. In [2], contrary to the promise of the title of the paper, the methods referred are mostly applicable for wireless ad-hoc networks and MANETs.

Before one attempts to detect an intrusion, it is important to understand the nature and variation of attacks. The work by Martin Antonio [5] provides a fairly good analysis of MANET specific attacks and risk analysis by identifying assets, vulnerabilities and threats, usable for future MANET deployments and security work. Consequently, security solutions with static configuration would not suffice, and the assumption that all nodes can be bootstrapped with the credentials of all other nodes would be unrealistic for a wide range of MANET applications [3]. In practice, it is not possible to build a completely secure MANET system in spite of using the most complex cryptographic technique or so-called secured routing protocols. Some of the IDS algorithms that have been developed for MANETs are explained below. A comparative study is provided at the end of this section.

IDSX [1] was a cluster-based solution which used an extended architecture. The proposed solution acted as a second line of defence. Individual nodes could implement any IDS solution. IDSX was compatible with any IDS solution acting as the first line of defence. Simulation results show that the IDSX solution hardly produced any false positives. This was because it formed a consensus of the responses from different individual IDS solutions implemented in the nodes. Anomaly-based intrusion detection schemes could be deployed as the first line of defence. The proposed approach in [1] works within preset boundaries. In general, these are quite feasible and practical enough considering the nature of ad hoc networks. However, some of these may also be considered as the limiting constraints. IDSX has not been compared with any of the existing IDS solutions. Also, the proposed two-step approach would make the task of intrusion detection expensive in terms of energy and resource consumption.

In another innovative approach in [7], a solution is proposed using the concept of unsupervised learning in Artificial Neural Networks using Self-Organizing Maps. The technique named eSOM used a data structure called U-matrix which was used to represent data classes. Those regions which represented malicious information were watermarked using the Block-Wise method. Regions representing the benign data class was marked using the Lattice method. When a new attack is launched it causes changes in the pixel values. eSOM and the Watermarking technique can together identify if any pixel has been modified. This makes it very sensitive towards detecting intrusions. The authors claim that the solution is 80% efficient and remains consistent even with variations in mobility. Mentioned below are some of the drawbacks of this work [7]. The IDS employing eSOM would be trained in regular time periods. This results in additional overhead and takes a toll on the energy efficiency of the algorithm. However, the proposed intrusion detection engine has not been employed on various routing protocols for the detection of various types of attacks.

A leader election model for IDS in MANET based on the Vicky, Clarke and Groves (VCG) model was suggested in [8]. This requires every node to be as honest as possible. Leaders are elected in a manner which results in optimal resource utilization. Leaders are positively

rewarded for participating honestly in the election process. By balancing the resource consumption amongst the nodes, a higher effective lifetime of the nodes was achieved. Experimental results indicate that the VCG model performs well during leader election by producing a higher percentage of alive nodes. However, the simulation results indicate that the normal nodes will carry out more duty of intrusion detection and die faster when there are more selfish nodes. Besides, as selfish nodes do not exhaust energy to run the IDS service, the percentage of packet analysis decreases with time. This is a severe security concern. In the case of static scenarios, the model elects the same node as leader repeatedly. This causes the normal nodes to die very fast.

CONFIDANT, another approach, similar to Watchdog and Path-rater scheme, has been proposed to overcome the drawbacks of the Watchdog and Path-rater by ignoring misbehaving nodes in the routing process [9]. Every node identifies its neighbours as friends and enemies, based on trust. Friends are informed of enemies. CONFIDANT claims that the packet delivery ratio is very high (97% and above). A couple of the issues that still leaves a gap in [9] are mentioned below. However, CONFIDANT keeps the packet delivery ratio high even in a very hostile environment, with the assumption that enough redundant paths are available to reach the destination node, bypassing the malicious ones. This assumption may not always hold. Also, in comparing the throughput of clients and servers, the CONFIDANT fortified network performs very poorly in contrast to the benign network.

SCAN [10] is based on two central ideas. First, each node monitors its neighbours for routing or packet forwarding misbehaviour, independently. Second, every node observes its neighbours by cross validating the overhead traffic with other nodes. Nodes are declared malicious by a majority decision. This assumes that the network density is sufficiently high. However, in SCAN the network services are temporarily halted during intrusion detection. The lack of mobility reduces the detection efficiency. The assumption that network density is high may not always hold. Increase in mobility results in higher false positives. Besides, the packet delivery ratio can be heavily affected in the interval during which an attack is launched and when it is detected. Also, the communication overhead for SCAN grows with increase in the percentage of malicious nodes and with mobility.

In HIDS [3], another approach to the IDS has been proposed. HIDS is based on trust or reputation or honesty values of the mobile nodes. The trust value of a node is dynamically increased or decreased depending on its behaviour. When a node behaves normally, it is positively rewarded; malicious activity results in negative rewards for that node. The trust on a node is recomputed based on its current honesty rate, and the rewards that it has earned. A comparative study between SCAN and HIDS shows that the latter involves lower storage and communicational overhead than SCAN. HIDS is inherently protected against false positives. However, maintaining up-to-date tables at different nodes, as required by HIDS, may not be an energy-efficient strategy. Also the proposed HIDS offers only a generic architecture for secure route detection. More detailed testing is required before it can be used for secure routing in MANET applications.

In [16] OCEAN was proposed as another extension to the DSR protocol. OCEAN also uses a monitoring system and a reputation system. The proposed solution exchanges second-hand reputation messages. OCEAN implements a stand-alone architecture to avoid phantom intrusion detections. Depending on whether a node participates in the route discovery process, OCEAN can detect misbehaving nodes and selfish nodes. However, the detection efficiency of OCEAN rapidly decreases with increase in the density of misbehaving nodes. Simulation results show that at high threshold values, other second hand protocols perform better with high mobility of the nodes. Also, the mobility model simulated for OCEAN is not very realistic. At high

mobility, OCEAN is very sensitive to change of the threshold parameter, while second hand protocols are more consistent over varying threshold limits. OCEAN is not quite effective in penalizing misleading nodes.

A hybrid solution, proposed in [17], combines the Watchdog and Path-Raters scheme proposed by Marti et al. and SCAN [10]. However, neither SCAN nor Watchdog and Path-raters address the mobility issue that well. As a result, this hybrid solution also suffers from the same problems. Besides, there are no fixed nodes which can behave as umpires. There must be some kind of a leader election model which runs in every node to select the Umpire nodes. This results in an increased overhead and energy consumption. The authors did mention the scenario where Umpire nodes themselves can become malicious. However, it still remains as a drawback of the method. In order to detect DoS attacks like flooding, the criteria for attack detection cannot be so rigid. Also, the history of a node that had being behaving normal, should be taken in to consideration before writing it off as malicious as soon as it deviates from normal behaviour.

Table 2. Summary on Comparison for Different IDS for Mobile Ad-hoc Networks

IDS Reference	**Under-lying Routing Protocol**	**Architecture**	**Types of attacks addressed**	**Comments**
IDSX [1] (2007).	Compatible with any routing protocol	Extended Hierarchical Architecture	Routing misbehaviour - dirty packet forwarding.	• The solution talks about a two-step approach. This leads to making the intrusion detection approach quite expensive in terms of energy and resource consumption.
Neural Networks and Watermarking Technique [7] (2007)	AODV	Self Organizing Maps (Neural Networks)	Routing behaviour attack and Resource utilization attack.	• The IDS using eSOM needs to be trained in regular interval. This additional overhead affects the energy efficiency of the algorithm. • The proposed intrusion detection engine has not been employed for various routing protocols for detection of different attacks.
CONFIDANT [9] (2002)	DSR	Distributed and Cooperative.	Packet drop attack.	• CONFIDANT assumes that there are enough nodes to provide harmless alternate partial paths around malicious nodes. This may not always hold. • A CONFIDANT fortified network with one third malicious nodes does not provide any additional benefits over a regular benign DSR network without malicious nodes.
HIDS [3] (2008)	Compatible with reactive And proactive routing protocols.	Distributed and Collaborative	Packet drops, black-hole attack, Resource utilization attacks	• Maintenance of tables at different nodes affects energy efficiency and communication overhead. • Detailed testing is required before it can be used for secure routing in MANET applications.
Leader Election Model [8] (2008)	Not specified.	Vickey, Clarke, and Groves (VCG) model by which truth-telling is the dominant strategy for each node.	Resource utilization attack-selfish nodes.	• Simulation results indicate that normal nodes will work more to detect intrusion and die faster in presence of selfish nodes. • As selfish nodes do not exhaust energy to run the IDS service, the percentage of packet analysis decreases with time. • In the case of static scenarios, the model elects the same node as leader repeatedly. This causes the normal nodes to die very fast.
SCAN [10] (2006)	AODV	Distributed and Collaborative	Routing misbehaviour and packet	• Network services are temporarily halted during intrusion detection. • Lack of mobility reduces the detection

			forwarding misbehaviour	efficiency. • The assumption that network density is high may not always hold. Increase in mobility results in higher false positives. • Packet delivery ratio can be heavily affected in the interval between an attack is launched and when it is detected. • The communication overhead steadily increases with increase in the percentage of malicious nodes and with mobility.
OCEAN [16] (2003)	Not identified	Stand - alone IDS	Routing behaviour attack, resource utilization attack, rushing attack.	• At high faulty thresholds, approaches like SEC-HAND protocols are able to perform better than OCEAN at high mobility. • At lower numbers of misbehaving nodes, the performance of OCEAN falls drastically. • OCEAN is not very effective in thwarting the throughput of the misleading nodes.
A System of Umpires [17] (2010)	Not identified	Stand - alone IDS for single user; Collaborative IDS for double and triple Users	Routing misbehaviour attack and Packet Dropping attack.	• Umpires are not static. Some kind of leader election is required. This may require additional energy. • Attack detection criteria are very rigid. • Nodes are not rewarded for normal behaviour.

4. IDS FOR WIRELESS SENSOR NETWORKS

The absence of a central entity made the detection of attacks a very difficult problem, since highly dynamic large networks cannot be easily monitored. Benign failures, such as transmission impairments, path breakages, and dropped packets, were naturally a fairly common occurrence in mobile ad hoc networks, and, consequently, malicious failures would be more difficult to distinguish. Moreover, abnormal situations occurred frequently because nodes behaved in a selfish manner and did not always assist the network functionality. It was noteworthy that such behavior may not be malicious, but only necessary when, for example, a node shuts its transceiver down in order to preserve its battery [29]. Thus, from obvious reasoning, it can be anticipated that providing an infrastructure to Ad-Hoc Networks had become the need of the hour. A significant advancement in networking environments was Sensor Networks where a base station has been added to an otherwise ad-hoc network.

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges [20]. The low cost allows a massive deployment of thousands of nodes in large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. Indeed, as pointed out in [30], wireless sensors often have the processing characteristics of machines that are decades old (or longer), and the industrial trend is to reduce the cost of wireless sensors while maintaining similar computing power.

With this in mind, many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. All aspects of the wireless sensor network are being examined including secure and efficient routing [29, 31, 32], data aggregation [33, 34], group formation [35, 36], and so on. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security [37]. Some of the existing protocols in Sensor Networks have been discussed briefly.

"SPINS: Security Protocols for Sensor Networks" was proposed in the year 2001. SPINS is perhaps the earliest security protocol that addresses the challenges of Sensor Networks. SPINS has two building blocks – namely the sensor network encryption protocol (SNEP) and μTESLA – to provide security services [30]. Some good Properties of SNEP include Semantic Security, Data Authentication, Replay Protection, Weak Freshness – If the message verifies correctly, a receiver knows that the message must have been sent after the previous message it received correctly and Low Communication Overhead. For SNEP and μTesla together, crypto library and protocol implementation consume about 2KBytes of program memory, which is quite acceptable in most applications. The amount of work needed for μTesla is easily performed by sensor nodes. The performance of the cryptographic primitives is adequate for the bandwidth supported by current generation of sensor networks.

In the year 2008, an efficient and distributed solution to the node capture attack has been proposed. In particular, they introduced two solutions: SDD, which does not require explicit information exchange between the nodes during the local detection, and CCD, a more sophisticated protocol that uses local node cooperation in addition to mobility to greatly improve performance. Experimental results shows that CDD requires less than 2000 seconds to detect node capture, which is much less than the benchmark. These results support the idea that node mobility, in conjunction with a limited amount of local cooperation, can be used to detect emergent global properties. The minimum detection probability of SDD is less than that of CDD. The number of false positives for both the SDD and CDD is influenced by NALM (number of alarms needed for revocation) and less influenced by MIT (Maximum Interval Time). The energy cost of CDD is less than the cost of SDD.

A game theory-based approach to intrusion detection was presented and discussed in [38] and [39] in 2004. In this framework, intrusion-detection is looked at in the form of a 2-player non-cooperative nonzero-sum game. The two players are the intrusion detection system (IDS) of the WSN, and the attacker. The IDS wants to maintain functionality of the network by preventing attacks, while the attacker wants to disturb normal operation. The model for the WSN is a large network of nodes sorted into clusters. When the IDS defends, it defends a cluster. Due to system limitations, the IDS can only defend one cluster at a time. The attacker can also only attack one cluster at a time. The justification for the first assumption is that the profit of the attacker should be related to the potential loss of the IDS. This metric may not be the best to use. The second assumption is based on the fact that if waiting were better than attacking, there would be no attacker. The final assumption is based on the idea that it is more costly to defend clusters that have been attacked before. Clusters that have been attacked have wasted some energy (due to extra transmissions or computations to defend). This game formulation is rather unsatisfying. There are a few obvious problems with it. First, the attacker benefit is independent of what the IDS do. But if the attacker's goal is to cause harm to the network, it should derive greater utility if the IDS does not defend against the attack. Secondly, the IDS should not have to defend only one cluster. If only one cluster could be defending at any given time, many extra control messages would have to be sent to coordinate the clusters. Plus, there could be a benefit to defending more than one cluster. It would just cost more resources.

In 2008 another Intrusion Detection system for both Homogeneous and Heterogeneous Wireless Sensor Networks was proposed [41]. This paper also considered two sensing models – single-sensing detection and multiple-sensing detection. According to the authors this paper was the first to address the issue of intrusion detection in heterogeneous sensor networks. This paper also defined the network connectivity and broadcast reachability in a heterogeneous WSN. The results showed that the intrusion detection probability is improved for heterogeneous sensor networks than homogeneous networks for both single-sensing detection and multiple-sensing

detection. But the results did not consider the effect of energy consumptions of the nodes and also the effect of intruder density on the intrusion detection system was ignored.

In 2009 a generic algorithm for cooperative intrusion detection system was proposed for Wireless Sensor Networks [40]. This cooperative intrusion detection system exploits the inherent redundancy of sensor nodes. The assumption that only one node was attacked by an intruder at one time, made this system quite weak for such scenarios where an attacker can attack more than one node at a time. This method is also time consuming, since the decision was taken collectively, based on the voting of honest nodes. Honest nodes also used the key exchange method to authenticate each other.

Another distributive approach called LIDeA [42] was proposed in 2008. This method was based on the fact that each node overhears its neighbors, and then a collective decision was taken to detect the intruder. This method was vulnerable to message lost. The system assumed that an intruder can completely take over nodes and extract their cryptographic keys, but such an adversary cannot "outnumber" legitimate nodes by replicating captured nodes or introducing new ones in sufficiently many parts of the network. The successful implementation of this proposal based on the fact that the time needed by an intruder to attack a node should be greater than the time required for the completion of the initialization phase, so that the initialization phase runs uninterrupted by malicious nodes. The topology of the network cannot change during this phase. The system also assumed that the attacker cannot introduce its own nodes in the network.

Table 3. Summary on Comparison for Different IDS for Wireless Sensor Networks

IDS Reference	**Under-lying Routing Protocol**	**Architecture**	**Types of attacks addressed**	**Comments**
SPINS: Security Protocols for Sensor Networks (2001).	Not specified.	Distributed Architecture.	Misbehaviour of a Node	• Information leakage through covert channels. • Compromised sensors are not dealt with completely. • Denial of Service (DoS) attacks have not been dealt with in this work. • Diffie-Hellman style key agreement or digital signatures have not been used to achieve non-repudiation. • μTesla requires buffering at sensor nodes that are extremely strained in terms of memory.
Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks (2008).	Not specified.	Distributed Architecture.	Node capturing attack	• Protocol behaviour has not been studied in the absence of an authentication mechanism. • It has been assumed that the only way to access/ modify the memory of a node is first to remove the sensor from the network, and then to tamper with it.
Preventing DoS attack in Sensor Networks: A Game Theoretic Approach (2004).	Utility based Dynamic Source Routing (UDSR)	two-player, nonzero-sum, non-cooperative game theoretic approach.	two types of DoS attack: black holes and falsify route error message	• Non-linear function for the utility value has not been explored. • False labelling • Setting appropriate threshold values. • The attacker benefit is independent of what the IDS does. • The IDS defends only one cluster at a time.
LIDeA: A Distributed	Not specified.	Distributed Architecture.	Malicious Behaviour of	• This method was vulnerable to message lost.

Lightweight Intrusion Detection Architecture for Sensor Networks (2008).			a Node	• Intruder cannot "outnumber" legitimate nodes by replicating captured nodes or introducing new ones sufficiently in different parts of the network. • The time needed by an intruder to attack a node needs to be greater than the time required for the completion of the initialization phase, so that the initialization phase runs uninterrupted by malicious nodes. • The topology of the network cannot change during this phase. • The attacker cannot introduce its own nodes in the network.
Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks (2008)	Not specified.	Distributed and collaborative Architecture.	Misbehaviour of a Node	• Did not consider the effect of energy consumptions of the nodes. • The effect of intruder density on the intrusion detection system was ignored.
Cooperative Intrusion Detection in Wireless Sensor Networks (2009)	Not specified.	Distributed and collaborative Architecture.	Malicious Behaviour of a Node	• All nodes that behave according to the protocol (honest nodes) are connected via a path consisted only of other honest nodes. • Only one node can be attacked by the attacker. • Did not consider the dynamic neighborhood changes, in particular, • into secure node addition and removal in sensor networks.

5. IDS FOR WIRELESS MESH NETWORKS

The proposed methodology successfully detects any moving object maintaining low computational complexity and low memory requirements.

Although mobility of nodes was removed and a certain infrastructure was established for Sensor Networks, yet these remained vulnerable to security threats. Researchers realized that mobility is a feature which cannot be compromised with as it provides tremendous flexibility to end users. Yet, retaining an infrastructure would definitely be helpful. All these underlying observations led to the conclusion that a different type of network must be designed which incorporates both the mobility of clients and a basic infrastructure. This had been a major driving factor behind the inception of Wireless Mesh Networks.

Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs [2]. They provide network access for both mesh and conventional clients. The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. WMNs include mesh routers forming an infrastructure for clients that connect to them. The WMN infrastructure/backbone can be built using various types of radio technologies. The client meshing provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end user applications to customers. Hence, a mesh router is not required for these types of networks. In Client WMNs, a packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMNs are usually formed using one type of radios on devices. Moreover, the requirements on end-user devices is increased when compared

to infrastructure meshing, since, in Client WMNs, the end-users must perform additional functions such as routing and self-configuration.

Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid architecture will be the most applicable case in our opinion.

The redundancy and self-healing capabilities of WMNs provide for less downtime, with messages continuing to be delivered even when paths are blocked or broken. The self-configuring, self-tuning, self-healing, and self-monitoring capabilities of mesh can help to reduce the management burden for system administrators. Besides, the advanced mesh networking protocols coordinate the network so that nodes can go into sleep mode while inactive and then synchronize quickly for sending, receiving, and forwarding messages. This ability provides greatly extended battery life.

A mesh network can be deliberately over-provisioned simply by adding extra devices, so that each device has two or more paths for sending data. This is a much simpler and less expensive way of obtaining redundancy than is possible in most other types of networks. In comparison to the cost of point-to-point copper wiring and conduit required for traditional wired networks, wireless mesh networks are typically much less expensive. The protocols that have been developed so far for WMNs are described briefly. A comparative study is provided at the end of this section.

A technique was devised based on the communication history between two communicating clients through a common set of routers in [15]. Individual trust relationships are evaluated for both clients sharing the common set of routers. Malicious clients are detected based on threshold values. The algorithm performs well when the density of malicious nodes is low. Routers in the path have to perform $O(N^2)$ operations to cooperatively reach a conclusion. It is found that false positives are reduced to a great extent but not eliminated. The algorithm performs better only when the percentage of misbehaving clients is smaller. Performance degrades as malicious activity within the network increases.

RADAR [12] introduces a general concept of reputation. Highly detailed evaluation metrics are used to measure the behaviour of mesh nodes. This allows RADAR to better classify / distinguish normal behaviour from anomalous activity. RADAR takes into consideration the spatio-temporal behaviour of nodes before declaring them as malicious. Simulation results show that RADAR detects routing loops with higher false alarms. The algorithm is resilient to malicious collectives for subverting reputations; but involves a relatively high latency for detection of DoS attacks. The Detection Overhead Ratio (DOR) is directly proportional to the number of anomaly detectors and the size of detection window implemented in the algorithm.

Although developed initially for wired networks, Principal Component Analysis (PCA) based method [11] could also be implemented for wireless networks. The threshold value used in [11] for detecting malicious nodes assumes that network traffic follows the normal distribution. Tuning the threshold also reduces the number of phantom intrusion detections considerably. The proposed solution is energy-efficient. However, despite the promises, the PCA based method in [11] is not consistent to variations in normal network traffic due to unrealistic assumptions in the method. Anomalies such as node outages cannot be detected as this method [11] looks for spurious traffic generation. A statistical analysis of how the behaviour varies with changing threshold values is yet to be performed.

In [14] a solution to defend against selective forwarding attacks based on AODV routing protocol is presented. The algorithm works in two phases – detecting malicious activities in the network and identifying the attacker, respectively. However, the proposed methodology of [14] suffers from some serious limitations. The proposed scheme fails to detect attackers when the threshold value is less than the throughput. Even in the absence of an attacker, the throughput is low when the detection threshold is higher than throughput of the path. The overhead of the system increases with increase in the density of malicious nodes.

OpenLIDS [13] analyzes the ability of mesh nodes to perform intrusion detection. Due to the resource constraints of mesh nodes, detailed traffic analysis is not feasible in WMNs. An energy – efficient scheme was proposed in OpenLIDS. Results show that performance improved for detecting malicious behaviour in mesh nodes. OpenLIDS is an improvement over other signature-based approaches both in terms of memory requirements and packet delivery ratio. However, simulation results show that OpenLIDS is unable to distinguish an RTP stream from a UDP DoS flood with fixed source and destination ports. For new connections, this approach is not as efficient as expected as generating and receiving connection tracking events is costly.

In [6], a framework has been proposed that is based on a reputation system. This isolates ill-behaved nodes by rating their reputation as low, and distributed agents based on unsupervised learning algorithms, that are able to detect deviations from the normal behaviour. The solution is very effective in detecting novel intrusions. This algorithm had already been deployed for WSNs. Experimental results show that even though redundancy reduces drastically in WMNs the proposed method works efficiently. However, the approach is not fast enough to prevent the neighbour nodes from being affected by an attack. Also, initially the solution [6] cannot exactly determine the source of the anomaly. Therefore, the system reduces the reputation of all the nodes within the malicious region.

Table 4. Summary on Comparison for Different IDS for Wireless Mesh Networks

IDS Reference	Under-lying Routing Protocol	Architecture	Types of attacks addressed	Comments
Trust based approach I [14] (2008).	AODV	Distributed System	Gray hole attacks.	• The overhead of the system increases with the number of attackers. • When detection threshold is less than the throughput of a path, attacks will not be detected and network throughput will suffer. • On the contrary, when the detection threshold is higher than throughput of the path, the throughput would suffer even if there is no attacker.
Trust based approach II [15] (2008)	Not specified.	Distributed Systems	Misbehaviour of a node	• The detection efficiency decreases and false positive rate increases with the increase of percentage of malicious clients. • False positives are reduced to a great extent but not eliminated.
Principal Component Analysis (PCA) [11] (2008).	Not specified	Distributed Systems	DoS, port scan, jamming etc.	• Anomalies such as node outages are not detected as the method looks for spurious traffic generation. • Analysis on performance evaluation with changing threshold values is yet to be performed. • The method is not consistent due to unrealistic assumptions on network traffic.

RADAR [12] (2008).	DSR	Distributed Systems	Malicious behaviour of a node, DOS Attack, Routing Loop Attack.	• Higher false alarms. • Resilient to malicious collectives for subverting reputations. • High latency for detection of DoS attacks. • The Detection Overhead Ratio (DOR) is a linear overhead.
OpenLIDS [13] (2009).	Not specified	Distributed Systems	Resource starvation attacks, mass mailing of internet worms, IP spoofing.	• Higher false positives as OpenLIDS is unable to distinguish between RTP stream and a UDP DoS flood with fixed source and destination ports. • Not as efficient for new connections. • It is not possible to arbitrarily adjust timeout values.
Reputation systems and self-organizing maps. [6] (2010).	Not specified.	Distributed agent based Systems	Routing misbehaviour and resource utilization attacks.	• It is assumed that the confidentiality and integrity cannot be preserved for any node. • The reputation system identifies the attacked node immediately. However, it is not fast enough to prevent the neighbor nodes from being affected

6. CONCLUSIONS

The infrastructure-less wireless ad-hoc networks holds a great potential to realize a plethora of applications. One could not even possibly imagine such use of technology with a conventional network. We get to know about such exciting applications from periodicals and journals on ubiquitous computing, ambient intelligence, next-generation networking, etc. However, so far only a small fraction of these have been implemented and even fewer are made commercially available to end users. One of the major bottlenecks between the theoretical potential and its practical realization is the concern for security. The flexibility that the wireless ad-hoc networks offer is like a double-edged knife that leaves an equal opportunity to the intruder as well the true user. In this paper, a comprehensive review has been done on the passive security mechanism of intrusion detection system (IDS) for different types of wireless ad-hoc networks. More than fifty different IDS approaches have been cited in this paper. It becomes practically impossible to experimentally evaluate or even simulate such large number of distinct approaches. Thus a qualitative comparison has been documented for different IDS solutions classified in the four major wireless ad-hoc network categories. The current study may be extended to review recent works on cross-layer IDS architecture, security for under-water ad-hoc networks, etc. These have been kept beyond the scope of the present article.

REFERENCES

[1] R. Chaki, N. Chaki; "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2007.

[2] Thomas M. Chen, Geng-Sheng Kuo, Zheng-Ping Li, and Guo-Mei Zhu, “Intrusion Detection in Wireless Mesh Networks”; Security in Wireless Mesh Networks, CRC Press, 2007.

[3] P. Sil, R. Chaki, N. Chaki; "HIDS: Honesty-rate based collaborative Intrusion Detection System for Mobile Ad-Hoc Networks", Proc. of 7th IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2008.

[4] S. Sahu, S. K. Shandilya, “A Comprehensive Survey on Intrusion Detection in MANET”, Int'l J. of Information Technology and Knowledge Mgmt., vol. 2(2), pp. 305-310, 2010.

[5] Antonio Martin, "A Platform Independent Risk Analysis for Mobile Ad hoc Networks", Proc. of the Boston Univ. Conference on Information Assurance and Cyber Security, 2006.

[6] Zorana Bankovic, et. al., “Improving security in WMNs with reputation systems and self-organizing maps”, Journal of Network and Computer Applications, ISSN 1084-8045, 2010.

[7] Aikaterini Mitrokotsa, Nikos Komninos, Christos Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," International Conference on Pervasive Services, pp. 118-127, IEEE Int'l Conference on Pervasive Services, 2007.

[8] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, Prabir Bhattacharya, Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[9] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, 2002.

[10] H. Yang, J. Shu, X. Meng, S. Lu, "SCAN: self-organized network-layer security in mobile ad hoc networks," IEEE J. on Sel. Areas in Communications, vol. 24, pp. 261-273, 2006.

[11] Zainab R. Zaidi, Sara Hakami, Bjorn Landfeldt, and Tim Moors, "Detection and identification of anomalies in wireless mesh networks using Principal Component Analysis (PCA)", World Scientific Journal of Interconnection Networks (JOIN), 2008.

[12] Zonghua Zhang, Farid Naït-Abdesselam, Pin-Han Ho, Xiaodong Lin. "RADAR: A ReputAtion-Based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks", IEEE Wireless Communications & Networking Conference, pp. 2621-2626, IEEE, 2008.

[13] Fabian Hugelshofer, Paul Smith, David Hutchison, Nicholas J.P. Race, "OpenLIDS: A Lightweight Intrusion Detection System for Wireless Mesh Networks", MobiCom'09, September 20–25, 2009, Beijing, China, 2009.

[14] Devu Manikantan Shila, Tricha Anjali, "Defending Selective Forwarding Attacks in WMNs", Proc. of IEEE Int'l Conference on Electro/Information Technology, pp. 96-101, USA, 2008.

[15] Md. Abdul Hamid, Md. Shariful Islam, and Choong Seon Hong, "Misbehavior Detection in Wireless Mesh Networks", ICACT 2008, pp. 1167-1169, 2008.

[16] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," Research Report cs.NI/0307012, Stanford University, 2003.

[17] Ayyaswamy Kathirvel, Enhanced Triple Umpiring System for Security and Performance Improvement in Wireless MANETS, International Journal of Communication Networks and Information Security (IJCNIS), Vol 2, No 2 (2010)

[18] Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", Virginia Polytechnic Institute and State University, 2003.

[19] Z. Liang and W. Shi.; "Enforcing cooperative resource sharing in untrusted peer-to-peer environment"; ACM Journal of Mobile Networks and Applications (MONET), 10(6):771–783, 2005.

[20] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci; "A survey on sensor networks"; IEEE Communications Magazine, 40(8):102–114, August 2002.

[21] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking MobiCom'00), Boston, MA, August 2000, pp.255-265.

[22] A. Smith, "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks," 5th Nat'l, Colloq. for Info. Sys.Sec. Education, 2001.

[23] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.

[24] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003.

[25] L. Stamouli, P.G. Argyroudis, and H. Tewari, "Real-time Intrusion Detection for Ad hoc Networks," Proceedings of sixth IEEE International Symposium Computers and Communications, June 2005, pp.374

[26] Ian F. Akyildiz, Xudong Wang, Weilin Wang, Wireless mesh networks: a survey, Elsevier, 2004.

[27] Edith C. H. Ngai and Michael R. Lyu, Roland T. Chin, "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks", Proc. of IEEE Aerospace Conference, 2004, pp. 1275-1285.

[28] Z. Li, A. Das, J. Zhou; "Theoretical Basis for Intrusion Detection"; Proceedings of 6th IEEE Information Assurance Workshop (IAW), 2005.

[29] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing For Mobile Ad hoc Networks", Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS) , 2002.

[30] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler; "Spins: security protocols for sensor networks"; Wireless Networking, 8(5):521–534, 2002.

[31] J. Deng, R. Han, and S. Mishra; "INSENS: intrusion-tolerant routing in wireless sensor networks"; Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, 2002.

[32] B. Karp and H. T. Kung; "GPSR: greedy perimeter stateless routing for wireless networks"; Proc. of the 6th Int'l conf. on Mobile computing and networking, pp. 243–254, 2000.

[33] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar; "Next century challenges: Scalable coordination in sensor networks. In Mobile Computing and Networking, pp. 263–270, 1999.

[34] L. Hu and D. Evans; "Secure aggregation for wireless networks"; Proc. of the Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), 2003.

[35] A. R. Beresford and F. Stajano; "Location Privacy in Pervasive Computing"; IEEE Pervasive Computing, 2(1):46–55, 2003.

[36] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz; "Secure multicast groups on ad hoc networks"; Proceedings of the 1st ACM workshop on Security of Ad hoc and Sensor Networks (SASN '03), pages 94–102, ACM Press, 2003.

[37] S. Ganeriwal and M. Srivastava; "Reputation-based framework for high integrity sensor networks"; Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004.

[38] Afrand Agah, Sajal K. Das and Kalyan Basu, "A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks"

[39] Afrand Agah, Kalyan Basu and Sajal K. Das, "Preventing DoS attack in Sensor Networks: A Game Theoretic Approach".

[40] Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C. Freiling, and Tassos Dimitriou. "Cooperative Intrusion Detectionin Wireless Sensor Networks" EWSN 2009, LNCS 5432, pp. 263–278, 2009, Springer-Verlag Berlin Heidelberg 2009.

[41] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang, and Dharma P. Agrawal, "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks."

[42] Ioannis Krontiris, Thanassis Giannetsos and Tassos Dimitriou."LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks" SecureComm '08, September 22 - 25, 2008, Istanbul, Turkey.

[43] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, Nov-Dec. 1999.

[44] N. Asoka n and P. Ginzboorg, "Key-Agreement in Ad-hoc Networks", Proceedings of the Fourth NordicWorkshop on Secure IT Systems (Nordsec '99), 1999.

[45] Amitabh Mishra, Ketan M.Nadkami, "The Electrical Engineering Handbook Series, The handbook of ad hoc wireless networks", CRC Press, Inc. Boca Raton, FL, USA 2003, Pages: 499 – 549.

[46] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002), 2002.

[47] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, 40(8):102–114, August 2002.

[48] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing in wireless sensor networks", Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, 2002.

[49] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks", Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243–254, ACM Press, 2000.

[50] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Poster abstract secure locations: routing on trust and isolating compromised sensors in location aware sensor networks",

Proceedings of the 1st international conference on Embedded networked sensor systems, pages 324–325. ACM Press, 2003.

[51] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks", Mobile Computing and Networking, pages 263–270, 1999.

[52] L. Hu and D. Evans, "Secure aggregation for wireless networks", SAINTW '03: Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), page 384, IEEE Computer Society, 2003.

[53] A. R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, 2(1):46–55, 2003.

[54] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004.

[55] Z. Liang and W. Shi, "Analysis of recommendations on trust inference in the open environment", Technical Report MIST-TR-2005-002, Department of Computer Science, Wayne State University, February 2005.

[56] Novarun Deb, Manali Chakraborty, Nabendu Chaki, "A State-of-the-art Survey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks"; Springer Heidelberg Proceedings of the International Conference on Parallel, Distributed Computing technologies and Applications (PDCTA-2011), pp. 169-179, September, 2011. ISBN: 978-3-642-24036-2.

Authors

Novarun Deb, born in 1987 has completed his high-school studies in 2005 with approximately 96% of marks. He has done his Bachelors' in Computer Science Honours from the University of Calcutta in 2008 securing the top position in the University with an all-time record marks at that level. Subsequently he has completed M.Sc. from the same University in 2010 securing the top rank again. Novarun is currently doing M. Tech. in Computer Science and Engineering from the University of Calcutta. He was awarded with the Mamraj Agarwal Rasthriya Puraskar in August, 2011 for his excellent academic performance. He has already published a research paper in international forum.

Manali Chakraborty, born in 1988, completed her high-school in 2005 from the West Bengal Council of Higher Secondary Education, India. She her Bachelors' in Computer Honours from the University of Calcutta in 2008. In the same year she has enrolled in the M. Sc. Program in Computer and Information Science under University of Calcutta and completed the same in 2010. She is currently pursuing M. Tech. in Computer Science and Engineering from the same University. Manali is recipient of prestigious Taraksudha Fellowship and she is a visiting faculty member for under-graduate studies in Bethune College, Kolkata, India.

Nabendu Chaki is HoD and an Associate Professor in the Department Computer Science & Engineering, University of Calcutta, Kolkata, India. He did his first graduation in Physics and then in Computer Science & Engineering, both from the University of Calcutta. He has completed Ph.D. in 2000 from Jadavpur University, India. Dr. Chaki has authored a couple of text books and close to 100 refereed research papers in Journals and International conferences. His areas of research interests include distributed computing and software engineering. Dr. Chaki has also served as a Research Assistant Professor in the Ph.D. program in Software Engineering in U.S. Naval Postgraduate School, Monterey, CA. He is a visiting faculty member for many Universities including the University of Ca'Foscari, Venice, Italy. Dr. Chaki is a Knowledge Area Editor in Mathematical Foundation for the SWEBOK project of the IEEE Computer Society. Besides being in the editorial board for several International Journals, he has also served in the committees of close to 50 international conferences.