ISSN:0975-9646

HIDES: Hierarchical based and an Energy Efficient Intrusion Detection System for Wireless Sensor Networks

B Kamaladharan

M.Tech (CSE) Scholar,
Visvesvaraya Institute of Advanced Technology,
Muddenahalli, Chickaballapur,India

ABSTRACT- In the past few decades, the development in the field of wireless networks has changed the landscape of wireless communication and network security. This advancement has led to the development of low-power, low-cost sensor nodes that are considerably small in size and applicable in wire variety of applications like, tracking the movements of tanks and troops on the battlefields, tracking the navigation of ships and sub-marines in the sea, monitoring environmental phenomena like earthquakes, tsunamis, forest fire and also in the field of medicine and science. Hence the security of wireless networks has become a major concern, especially for the applications where confidentiality is of peak importance. While the traditional way of protecting the network with firewall and encryption techniques have proven to be insufficient for wireless networks, the need of more secure and scalable architecture of security has alarmed the requirement of Intrusion Detection System (IDS), which are applicable for wireless networks. In this project, Hierarchical based and Energy Efficient Intrusion Detection System has been implemented, which is more secure, scalable and energy efficient compared to other Intrusion detection Systems.

Key -terms: Hierarchical based IDS, Dynamic Hierarchy, Virtual Area Partition.

I. INTRODUCTION

The rapid innovation in the field of Wireless Sensor Networks (WSNs), has changed the landscape of wireless communication and network security. This advancement has led to the development of low-power, low-cost sensor nodes that are considerably small in size and applicable in wire variety of applications. Due to its easy to deploy features, it is a low cost solution to a wide variety of problems like, tracking the movements of tanks and troops on the battlefields, tracking the navigation of ships and sub-marines in the sea, monitoring environmental phenomena like earthquakes, tsunamis, forest fire, monitoring the activities at industrial sites, in the field of medicine and science and so on.

However, security has become one of the major concern that wireless network facing today. While the traditional method of securing the networks with firewall and cryptographic techniques have proven to be sufficient as the first line of defense for the wired networks, but insufficient in the case of wireless networks due to its lack of power and data storage facilities. Wireless networks are prone to eavesdropping, signal jamming, spoofing attacks and are susceptible to insecure communications. Hence the security of all the nodes in the network is of prime importance in order to preserve the integrity of overall network.

While the wireless nodes are low energy devices, they tend to die-off soon, when the amount of data processing and computations to be performed are of greater magnitude. Hence it demands for architecture for conserving the energy of the sensor nodes along with ensuring the security.

II. LITERATURE REVIEW

The next section presents a brief survey of different types of Intrusion Detection Systems proposed for WSNs in the literature and their possible outcomes.

A. Clustering (Hierarchical) based IDSs:

In the article [2], the authors proposed an approach with an isolation table to detect intrusions in hierarchical WSNs in an energy efficient way. In this approach, authors paid much importance two-levels of clustering. According to their experiment, their isolation table intrusion detection method could detect attacks effectively. The disadvantage with this proposal is that each level monitors the other level and reports any anomalies to the Base station. Since it is a hierarchical network, any alert generated by the lower level nodes must pass through the higher level nodes. If the higher level node happens to be an intruder, it will not allow the Base Station to be aware about its misbehavior by simply blocking the alert messages that it receives from the lower level nodes.

B. Distributed and collaborative IDSs:

In the article [3], the author proposed a Distributed IDS for WSNs based on collaborative neighborhood watching. In a simulation environment, the authors proved the effectiveness of their IDS scheme against selective forwarding attacks.

In [4], a solution to the problem of cooperative intrusion detection in WSNs was proposed, where the nodes were equipped with local intrusion detectors and has to identify the intruder in a distributed way. The detectors triggered suspicions about an intrusion in the sensor's neighborhood. The authors presented necessary and sufficient conditions for successfully exposing the attacker and a corresponding algorithm that is shown to work under a general threat model.

C. Statistical detection based IDSs:

In [5], the authors proposed an algorithm to detect the intruders in a sinkhole attack. The proposed algorithm first finds a list of suspected nodes and then effectively identifies the intruder in the list through a network flow graph. The algorithm implements a multivariate technique (statistical - parametric technique) based on the chi-square test. The accuracy of the proposed algorithm is verified by both numerical analysis and simulations. The authors claimed that their algorithm's

communication and computational overheads are reasonable for WSNs.

In the proposed algorithm of [6], the sensor network adapts to the norm of the dynamics in its surrounding so that any unusual activities can be identified. In order to achieve this, they employ a hidden Markov model. The authors claimed that their proposed algorithm is easy to employ, requiring minimal processing and data storage. The functionality and practicality of the algorithm is shown through experimental scenarios.

D. Game theory based IDSs:

In the articles [7] and [8], the authors proposed a game model that considered attack and detection as both participants of the game and formulated strategies for both the events. In order to increase the probability of detection, strategies were normalized into a non-cooperative game model. Both schemes focused on determining the weakest node in the network and then providing strategies to defend that node. The problem with this approach was that there might be multiple nodes as misbehaving nodes and only one of them would be caught by the IDS while leaving others undetected.

E. Anomaly detection based IDSs:

In [9], the same authors proposed a solution to the problem of minimizing the communication overhead in the network while performing in-network computation when detecting anomalies. Their approach to this problem is based on a formulation that uses distributed one-class quarter-sphere support vector machines to identify anomalous measurements in the data. Data vectors are mapped from the input space to a higher-dimensional space for further investigations. The authors implemented their proposal in a real-world project and they claimed that their model was energy efficient in terms of communication overhead while achieving comparable accuracy to a centralized scheme.

F. Watchdog based IDS:

In article [10], the author provided guidelines about application of IDSs (that are designed for MANETs) to static WSNs. Then, they proposed a detection algorithm for WSNs called ‘spontaneous watchdogs’ in which the neighbors are optimally monitored and where some nodes are configured to independently monitor the communications in their neighbor-hood.

G. Reputation (Trust) based IDS:

In the article [11], the author proposed an IDS for WSNs that uses packet marking and then heuristic ranking model to identify the nodes, that is likely to behave mischievous in the network. The packet mark is added in each packet such that the data sink can spot the source of the packet.

In the literature [12], the authors proposed a hierarchical trust model for WSNs to detect malicious nodes. Authors developed a probability model utilizing stochastic Petri nets technique to analyze the performance of the protocol. Their trust-based IDS algorithm outperforms anomaly-based IDS algorithms in the detection probability, while maintaining sufficiently making less use of system resource.

III. EXISTING SYSTEM

In the following a survey about the existing system and the problems concerning them are presented:

- In hierarchical, clustering based IDSs, the nodes may consume considerable amount of the network’s energy through the formation of the clusters. After the clusters are formed and once the CHs are being selected, CHs may become a single point of failure and due to which they have to be secured.
- Agent based IDSs reduces the overhead on network latency. On the other side, they cause high consumption of energy of the nodes. Communication overhead is induced between agents and coordinator, which may cause congestion and performance bottle neck in the network.
- Rule based IDSs are simple to install and easy to operate. However, they need continuous update of the network rule in order to cope with the new released attacks.
- Anomaly based IDSs can detect only unknown attacks. Unfortunately they have high computational complexity and high energy consumption requirement and require large amounts of data samples. Besides, they also need efficient analytic tools to analyze large amount of audit data and a mass memory space to store them.
- In game theory based IDSs, the detection rate can be varied by the network security administrator through changing the system parameters. The problem with this system is that it requires human intervention for a stable operation.

IV. PROPOSED SYSTEM

This section presents the proposed architecture for Hierarchical and energy efficient intrusion detection system. Under this we discuss, describes how the dynamic hierarchy facilitate intrusion detection.

A. The basic model- The Dynamic IDS hierarchy:

The choice of basic model is fundamental to the architecture of any distributed system. Common models include static hierarchy, peer-to-peer (P2P) and publish-and-subscribe. The static behavior of the static hierarchy model, the potentially huge volume of multi-hop traffic that may be generated as a result of the arbitrary information transfer in the peer-to-peer and publish and-subscribe models as well as assumptions of uniform trust in peer-to-peer model render them inappropriate for our problem domain

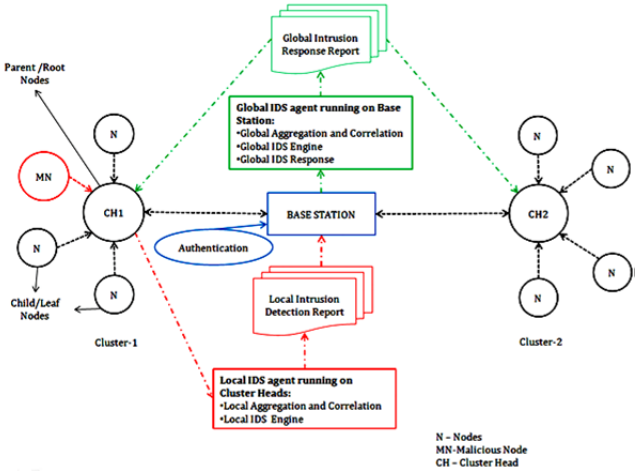

Fig 1: Hierarchical Intrusion Detection Architecture..

In order to facilitate an efficient and an incremental aggregation, detection, dissemination of intrusion management directives, scalability, and also to account for the energy efficiency of the model, the basic model that is being developed in this project is the dynamic hierarchy. The major advantage of a hierarchical based model is that, its potential scalability and rapid adaptability to large networks, since it can provide

communications-efficient detection for local attack recognition, while still allowing data sharing for more widely-distributed cooperative intrusion detection algorithms. Unlike P2P networks where communications burden can rise by the square of the number of nodes, a hierarchical approach allows higher-layer nodes to selectively aggregate and reduce intrusion detection data as it is reported upward from the leaf/child nodes to a parent/root. Moreover, a hierarchy dynamically aligns with the authority structure (chain-of-command) that is common to many human organizations. In the proposed architecture, this chain-of-command is represented by the flow of data to authoritative nodes at the root of the hierarchy, which dispatches to lower level nodes.

In this problem domain, mobility and other factors will cause the topology to change continually, such that an initially-defined static hierarchy will soon be inefficient. Hence a dynamic, hierarchical based topology must be deployed and constantly maintained. Nodes will communicate intrusion detection information most often with other nodes that are their parents or children in the hierarchy. Efficiency can be enhanced if children are topologically nearby, such as they are 1-hop away from one another. Since mobility and other factors will lead to frequent changes in these topological relationships, hierarchical relationships between nodes need to evolve as the topology evolves. We propose to use clustering technique for establishing and maintaining such a dynamic evolving hierarchy of intrusion detection components.

An example of this infrastructure is shown in Fig 2. Nodes annotated with number “1” are the representatives of level-1 clusters. This representative forms the Cluster Head (CH). Arrows pointing to these cluster head nodes originate from the other (child/leaf) nodes that belong to same cluster.

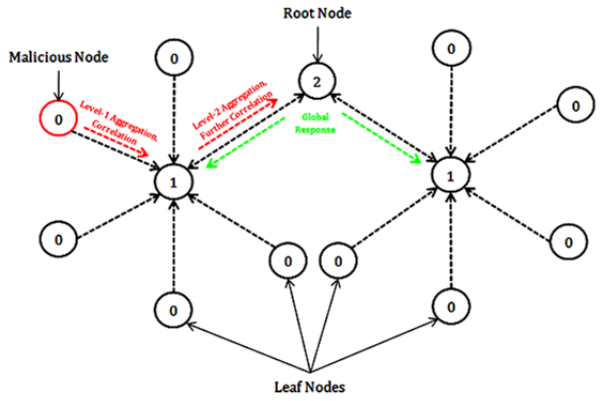

Fig 2: Dynamic Intrusion Detection Hierarchy

Likewise, arrows from first level nodes points to the level-2 representatives, (annotated with a “2) which forms the parent/root node. This representative forms the Base station. Other members of that cluster are outside the scope of the figure and are not shown. To avoid having a single representative node at the top of the hierarchy that is a potential single point of failure, one or more members of the level-1 cluster should be designated as backup representatives. This infrastructure allows intrusion detection reports to be collected efficiently from the entire network, providing incremental aggregation and correlation and efficient dissemination of intrusion response reports to all the lower level representatives.

V. SYSTEM IMPLEMENTATION

In this section, we present the pseudo-code for cluster formation algorithm followed by the method to construct dynamic hierarchy using Virtual Area Partition based clustering. We also describe here the responsibilities of nodes according to their placement within the hierarchy.

A. Cluster formation algorithm:

Clustering has important applications in sensor networks, because it is much easier to manage a set of cluster representatives (CH) from each cluster than to manage whole sensor nodes. In WSNs the sensor nodes are resource constrained which means they have limited energy, transmit power, memory, and computational capabilities. Energy consumed by the sensor nodes for communicating data from sensor nodes to the base station is the crucial cause of energy depletion in sensor nodes.
Advantages of clustering in WSNs:

- It enables to reuse the bandwidth and thus can improve the system capacity.
- Due to the fact that within a cluster, all the normal nodes send their data to the CHs so energy saving is achieved by absence of multiple routes or routing loops.
- Due to the fact that clustering enables efficient resource allocation and thus help in better designing of power control.
- Due to the fact that any changes of nodes behavior within a cluster affects only that cluster but not the entire network, which will therefore be robust to these changes.

In this project, a clustering algorithm which based on cell combination for the networks is been used. While Sensor nodes are distributed evenly in the space and the energy of sensor nodes is always random in each cluster, the transmission/reception power is considered constant for all the nodes in the cluster. In this clustering algorithm, the monitoring region is divided into virtual area partition (VAP) in heterogeneous networks environment and nodes appearing in each partition form a cluster and cluster head is selected based on the fact that the node having the highest energy within that cluster forms the cluster head. This technique enhances the energy efficiency of sensor nodes, improve the efficiency of communications, prolong the stability period and network life time with the same simulation condition.

With the basic foundation in place, the responsibilities of a node depend on its current positions in the topology, dynamic hierarchy as well as its energy. Nevertheless, data acquisition will generally occur at or near the bottom of the hierarchy where leaf nodes are attached. Intrusion detection data of all forms including alerts will generally flow upward and will be consolidated, correlated, and summarized incrementally as it flows upward. A key principle is that intrusion detection and correlation should occur at the lowest level in the hierarchy at which the aggregated data is sufficient to enable an accurate detection or correlation decision. If the data available at a level is not sufficient, it is pushed upward in the hierarchy where it is further aggregated with other data.

In our case, if the scenario is as such as if an intrusion is detected within a cluster, the CH in that cluster takes the responsibility of performing local intrusion detection and response activity. In another scenario in which, if the source happens to be an attacker, about which the CH has no much evidence to make a decision, the data is forwarded as normal to the CH. Further this flow continues up to the Base station (BS), where the data is aggregated and correlated and a global intrusion detection and response procedure is initiated. Under this process, each CHs are informed about the existence of an intruder(s) in each clusters in the network, including their Identification Number and the cluster in which that intruder(s) are found.

The Basic Algorithm:

The code below shows the sample TCL script for cluster formation algorithm using VAP method.

```
Set val(nn) No_of_Nodes
Source ./topology.tcl      ;# The x and y co-ordinates of all
the nodes are defined in this file

for {set i 0} {$i < $val(nn) } { incr i } {

        if {$x($i) > 200} {
                if {$y($i) > 200} {
                puts "The Node-$i is in cluster-1."
                                        }
                                }
        if {$x($i) > 200} {
                if {$y($i) < 200} {
                puts "The Node-$i is in cluster-2."

                                        }
                                }

        if {$x($i) < 200} {
                if {$y($i) < 200} {
                puts "The Node-$i is in cluster-3."
                                        }
                        }

        if {$x($i) < 200} {
                if {$y($i) > 200} {
                puts "The Node-$i is in cluster-4."
                                        }
                        }
}
```

Here we divide the simulation screen logically into four quadrants and compare the x and y co-ordinates of the each node with the simulation screen co-ordinates. The nodes appearing in any one of these quadrants is designated as a cluster. Likewise, we form four such clusters and designate them with four Cluster Identifiers.

B. Responsibilities of nodes in the network:

In this architecture, all nodes are responsible for their own protection including performing host-based intrusion detections and network based intrusion detection on network packets they generate. In addition, each node is responsible for additional set of task of intrusion detection responsibilities to help protect other nodes in the network. As described above, the responsibilities of a node depend, among other factors, on whether the node is currently acting as a cluster head and whether the node is currently in a topologically advantaged position to gather relevant observations.

1. Responsibilities of leaf nodes:

All leaf nodes in this architecture (nodes at the bottom of the detection hierarchy) are responsible for certain data acquisition, intrusion detection, and reporting functions. These include the following:

Link-Level Responsibilities– For each packet received, nodes records link-layer counts and statistics describing source and destination MAC addresses and type of transmitted and received packets. Each node reports these link-layer counts and statistics to its cluster head synchronously, asynchronously or as and when queried.

Infrastructure-Level Responsibilities– For each WSN infrastructure protocol packet received, nodes log packet headers and payloads. Each node forwards copies or summaries of WSN infrastructure protocol packets to its cluster head synchronously, asynchronously or as and when queried.

Network- and Higher-Layer Responsibilities– For specific packets that are received, each node also accumulates network and higher layer counts and statistics. These include

- Packets that are addressed to a particular node at the network layer, or
- Forward-able data packets belonging to end-to-end flows the node is currently responsible for monitoring.

For data flow assigned to a particular node, the node is required to perform conventional network layer, transport layer, and application layer intrusion detection processing. These responsibilities include,

- Recording reports and statistics on network and higher layer attributes such as source and destination IP addresses and port ID, protocols, packet lengths, and packet types and reporting these information to its cluster head synchronously, asynchronously or as and when queried.
- Performing signature matching or security violation checking on packet headers and payloads.
- If a signature match or specification violation occurs, logging all relevant evidence and sending an alert immediately to the node's cluster head.

2. Responsibilities of Cluster heads:

The responsibilities of cluster head nodes are much as like leaf nodes. In addition, a cluster head must perform the following tasks.

- Aggregate and consolidate its own intrusion detection data from the link, infrastructure, network, and higher layers with data reported by members of the cluster and perform intrusion detection computations on consolidated data.
- Recording reports and statistics on network and higher layer attributes such as source and destination IP addresses and port ID, protocols, packet lengths, and packet types and reporting these information to its base station synchronously, asynchronously or as and when queried.
- It also maintains the routing table, which consists of list of cluster head nodes, through which the report to be forwarded efficiently to the base station. The routing table usually contains the shortest path via which the report is forwarded.
- Like leaf nodes, e ach cluster head also reports intrusion detection data or data summaries, upward in the architecture to its own higher level node (Base station).

3. Responsibilities of Base station:

The responsibilities of base station are similar to that of cluster head. In addition, they have the authority and responsibility for configuring the detection and response capabilities of the nodes, clusters and cluster heads below them.

It performs the following tasks.

- Aggregate and consolidate its own intrusion detection data from the link, infrastructure, network, and higher layers with data reported by cluster heads and perform intrusion detection computations on consolidated data.
- Performing signature matching or security violation checking on packet headers and payloads that was received from the cluster head.
- If a signature match, specification violation, or any evidence of misbehaving node (intruder) is found from aggregated data, record all relevant evidences and send an alert/report immediately to all the cluster heads in the network about the presence of such a misbehaving node, even if that misbehaving node is a cluster head. This relinquishes the rest of the nodes in the network from the risk of being attacked from or accepting the packet from such Malicious Nodes.

VI. RESULTS

The simulation was conducted using the ns-2 Simulator Version 1.0a, which emulates a wireless ad hoc network on a local area network and thus enabling the measurement of various performance statistics.

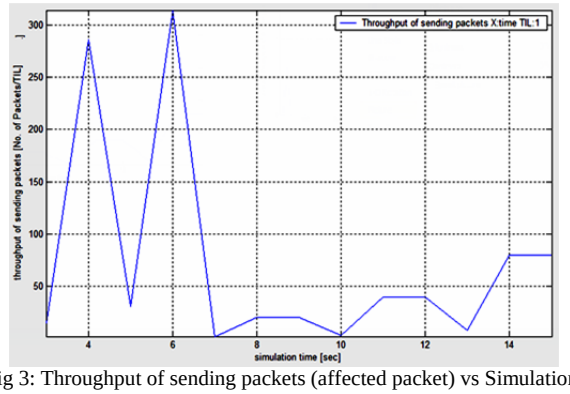

Fig 3: Throughput of sending packets (affected packet) vs Simulation Time

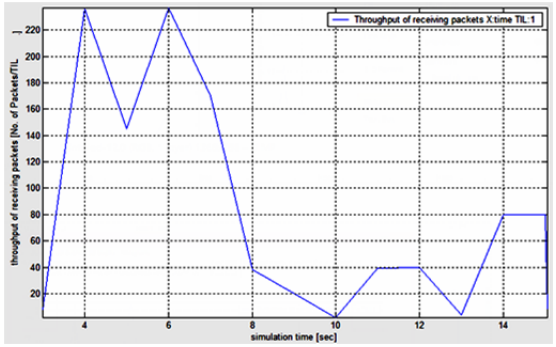

Fig 4: Throughput of receiving packets (Detected packets) vs Simulation Time

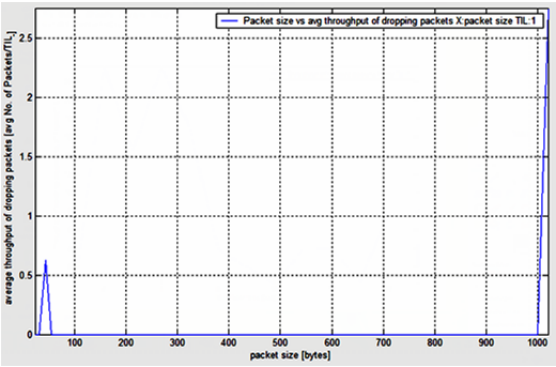

Fig 5: Average Throughput of dropped packets (False positive rate) vs Simulation Time

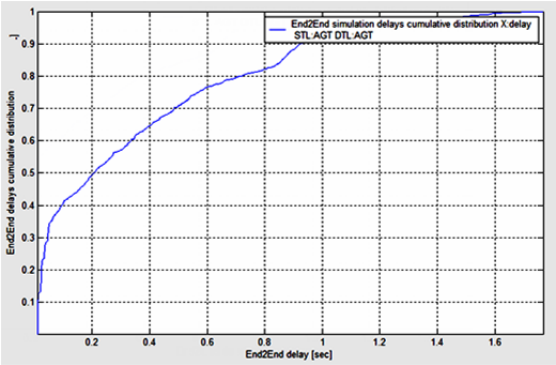

Fig 6: Average End to End simulation Delay (its less than 1 ms)

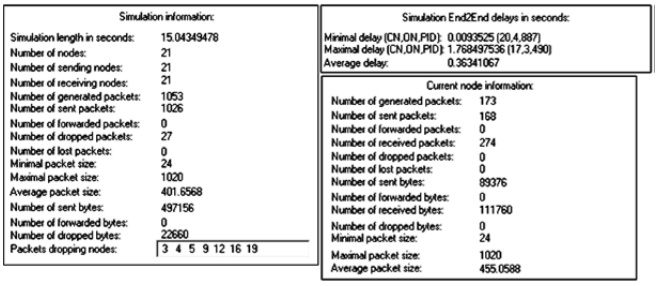

Fig 7: Showing the various statistics of the simulation.

The following criteria were then measured.

- **Throughput:** In this simulation, it can be defined as the number of packets successfully detected for any kind of intrusions.
- **Efficiency:** It is the maximum number of packets detected/processed in a given interval of time. (in 1 ms).
- **False positive rate:** It is the probability of giving a wrong alarm in an event of intrusion. In this project it is very less.
- **False negative rate:** It is the probability of giving a correct alarm in an event of intrusion. In this project it is very high.

VII. CONCLUSIONS AND FUTURE WORKS

In this project, a framework for Hierarchical based and energy efficient intrusion detection is being implemented. This framework is proven to provide high false negative rate, low false positive rates along with conserving the energy of the sensor nodes along with ensuring the security. Though intrusion cannot be completely eliminated, this framework is expected to eliminate some of the potential threat that would cause harm to the wireless networks.

As far as the future work is concerned, in a view to conserve the energy of the nodes and thus increasing the lifetime of the network, works are in progress to develop an algorithm that would extract and use the energy of the malicious nodes and distribute proportionally among the rest of the nodes in the network. This is a boost in terms of additional energy that can be used as a backup energy in case of emergency scenarios. This would automatically increase the lifetime of the nodes.

ACKNOWLEDGEMENT

I would like to thank our guide and our course coordinator Mrs. Nirmala Hiremani for her reviews and valuable comments regarding the preparation and editing of this paper.

REFERENCES

[1] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar,"A Survey of Intrusion Detection Systems in Wireless Sensor Networks", *IEEE communications surveys & tutorials, vol. 16, no. 1, first quarter 2014*

[2] R.C. Chen, C.F. Hsieh, Y.F. Huang, "A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", *in Proc. ACM ICUIMC-09*, 2009.

[3] I. Krontiris, T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks", *Proc. 13th European Wireless Conference*, 2007.

[4] I.Krontiris, Z. Benenson, T. Giannetsos, F. Freiling and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks", *Springer J. Wireless Sensor Networks*, pp. 263-278, 2009.

[5] E. Ngai, J. Liu and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," *ICC'06*, Istanbul, Turkey, June 2006.

[6] S.S. Doumit and D.P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks", *in Proc. IEEE Military Communications Conference (MILCOM'03)*, 2003.

[7] A. Agah, S.K. Das, K. Basu and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," *Proc. 3rd IEEE International Symposium on Network Computing and Applications (NCA'04)*, pp. 343-346, 2004.

[8] A. Agah and S.K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach", *International Journal of Network Security, volume 5, number 2*, pages 145-153, 2007.

[9] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Net-works", *IEEE ICC '07*, Glasgow, U.K., June 2007.

[10] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," *in Proc. IEEE Consumer Communications and Networking Conference*, 2006.

[11] C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, num. 5, pp. 835–843, 2012.

[12] F. Bao, R. Chen, M.J. Chang and J.H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", *IEEE Trans. Network Service Management*, vol. 9, num. 2, pp. 169–183, 2012.

[13] The network simulator, ns-2, cited in March 2015, available at: http: //www.isi.edu/nsnam/ns/

[14] I. Butun and R. Sankar, "A Brief Survey of Access Control in Wireless Sensor Networks," *in Proc. IEEE Consumer Communications and Networking Conference*, Las Vegas, Nevada, January 2011.

[15] Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari, IEEE Member, "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey," *IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011*.