Multiple Sensing Techniques for Intrusion Detection System in Heterogeneous Wireless Sensor Network

Kiruthika.S
AP/CSE
SCET,SGI
Villupuarm ,
India
Keerthis0209@gmail.com

Krishnaveni.S
Computer Science and Engineering
SCET,SGI
Villupuram,
India
sanjanaveni@gmail.com

Saranya.R
Computer Science and Engineering
SCET,SGI
Villupuram,
India
saransweety08@gmail.com

Abstract—**Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. Deploying sensors in open and unprotected environment in WSNs raises security issues. Various intrusion detection policies are developed till date to detect the nodes that are not working normally.we consider this issue according to two WSN models: homogeneous and heterogeneous WSN. Furthermore, we derive the detection possibility by considering two sensing models: single-sensing detection and multiple-sensing detection. The main categories explored in this paper are anomaly detection , misuse detection and specification based detection Focus of this paper is to detect the intruder in a given intrusion distance using multiple sensor in heterogeneous wireless sensor networks. It includes the most recent advancements in this area as well as to predict the future course of research so that the general as well as expert readers could be greatly benefited.**

Index Terms—Intrusion detection, wireless sensor networks, anomaly, misuse, specification-based.

I. INTRODUCTION

IN MANY WSN (Wireless Sensor Network) application scenarios security is a very important concern; especially the applications designed for WSNs deployed in hostile environments and commercial applications. With the level of importance of security in a WSN application, ensuring it to the expected level also becomes relatively more difficult than its other wireless network counterparts. In fact, security in WSN has a great number of challenges that may not be seen in other types of wireless networks. This is due to many reasons like the broadcast nature of wireless communications, limited resources of the sensor nodes, unattended environment where sensor nodes might be susceptible to physical attacks, etc. Security solutions like authentication, cryptography or key management can enhance the security of WSNs. Nevertheless, these solutions alone cannot prevent all possible attacks. As a wide range of attacks can be launched by compromised nodes in a WSN (i.e., nodes that appear to be legitimate in the network but not or working for other party, a second line of defense like Intrusion Detection System (IDS) is needed. An Intrusion detection system (IDS) is designed to detect unwanted attempts at accessing, disabling of computer mainly through a network, such as the Internet. Intrusion detection plays a key role in the vicinity of network security, so an attempt to apply the idea in WSNs makes a lot of sense. Intrusion, i.e. unconstitutional access or login (to the system, or the network or other resources); intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability.

A) Misuse detection: The action or behavior of nodes is compared with well-known attack patterns. In this case, these patterns must be defined and given to the system. The disadvantages are that this technique needs knowledge to build attack patterns and they are not able to detect novel attacks. In addition, always someone has to update the database of attack patterns. At current stage, most of the known attacks are only the results of some assumptions or imitated from other classic networks. Whether these well-known attacks or any unknown security attack would be a serious problem for sensor networks still remains unclear.

B) Anomaly detection**:** This technique does not search for specific attack patterns, but instead it checks whether the behavior of the nodes can be considered as normal or anomalous. The approach first describes the actual features of a ‘normal behavior’, which are established by using automated training. Afterwards, it flags any activities that deviate from these behaviors as intrusions. If a sensor node does not act according to the defined specification of a particular protocol, the IDS would have high confidence to decide that the node is malicious. The wrong decisions made by IDS in terms of false positive and false negative alarms affect the accuracy of detection. Hence, the disadvantage of this Also, an intrusion that does not exhibit a legitimate but unseen behavior, which could lead to a substantial false alarm rate. Also, an intrusion that does not exhibit anomalous behavior may not be detected, resulting in false negatives.

C)Specification based**:** This technique combines the aims of misuse and anomaly detection mechanisms, as it is focused on discovering deviations from normal behaviors that are defined neither by machine learning techniques nor by training data. In fact, the specifications that describe what can be considered as normal behavior are defined manually. Intrusion detection can be done in two ways: single sensing detection and multiple sensing detection. In single-sensing detection, the intruder can be successfully detected by one sensor. And the results of researches show that heterogeneous nodes can prolong network lifetime and improve network reliability without significantly increasing the cost. A typical heterogeneous wireless sensor networks consists of a large number of normal nodes and a few heterogeneous nodes.

II.RELATED WORKS

With respect to security, there are many tools that are used to ensure security in ID systems. The IDSs are very important tools since they can detect intrusions in networks. Many techniques that are result of research are pertaining to network security in general. They are developed for the nodes that have lot of resources in place. For this reason they can’t be directly applied to WSN. That led to further research in the area of WSN for modifying techniques or inventing new ones that are best suited for WSN where nodes are energy constrained. Their IDS which is distributed in nature works based on the detection techniques of statistical anomaly. This technique assumes much traffic and the time taken for detection of intrusion is high and thus not efficient. Most of the research that has been done in this area focuses on detection of intrusions under assumptions and criteria. Sensing models are of two types. They are single sensing model and multi sensing model. Intrusion detection process in these two models is explored by Wang et al. In his work, the combination of detection probability and network Parameters such as transmission range, sensing range, and node density are considered for experiments under single sensing model.

III. SECURITY THREATS AND TYPES OF ATTACKS IN WSN:

An attacker can exploit compromised nodes to launch many active attacks to disrupt normal operations in a WSN. Therefore, some detection methods must be performed to counteract these attacks.

A)Selective Forwarding — the forwarding packets is a major responsibility of a routing node. However, a malicious node intentionally may drop any packet and forward other ones. In their framework; each sensor node can work under a promiscuous mode so that it can overhear the transmission of neighboring nodes. If a neighbor of a suspected node finds that the number of packets that the suspected node fails to forward exceeds a certain threshold, the neighbor can collaborate with other neighbors of the suspected node, and the opinions from the neighbors of the suspected node are collected to form a decision about the suspected node.

B)The Sybil Attack — the *Sybil attack* was first studied in the context of peer-to-peer networks. In the Sybil attack a malicious node illegitimately takes on multiple identities. It has been shown that the Sybil attack may pose a serious threat to distributed storage and routing protocols. In addition, it also can cause devastating consequences to other applications such as data aggregation, voting, fair resource allocation, and misbehavior detection. Because the radio of a sensor platform is usually incapable of simultaneously sending or receiving on more than one channel, the failure of communication through one channel may be a sign of the Sybil attack. The other method is to use the ID-based symmetric keys. The ID of a suspected node is challenged by a set of validating nodes.

C)The Node Replication Attack — in the *node replication attack*, an attacker intentionally puts replicas of a compromised node in many places in the network to incur inconsistency. Where each node is assumed to know its location, and it is required to send its location to a set of witness nodes. Asymmetric key technology is used here to guarantee the authenticity of location claims.

D)The Wormhole Attack — In the *Wormhole attack,* an attacker can tunnel packets through a secret, low-latency broadband channel between two distant places and replay them. This attack can distort the network topology by making two distant nodes believe they are neighbors, thus it becomes a serious attack on routing protocols. To detect the Wormhole attack, we use *packet leashes, where* location or timing information is embedded in packets, to limit the maximum range over which packets can be tunneled. Location-based keys also can effectively address the Wormhole attack because each packet is authenticated by the location-based key.

E)The Rushing Attack — most on-demand routing protocols rely on broadcast ROUTE-REQUESTs to find routes. In a *rushing attack*, an attacker can forward ROUTE-REQUESTs more quickly than legitimate nodes so that it is more possible that the chosen route includes the adversary. The widely used duplicate suppression technique makes the rushing attack possible. To counteract the attack, Hu, Per rig, and Johnson proposed the Route Access Protocol (RAP), in which cached ROUTE-REQUESTs and the node lists embedded in those ROUTE-REQUESTs can be used to check the rushing attack.

IV.SYSTEM DESIGN

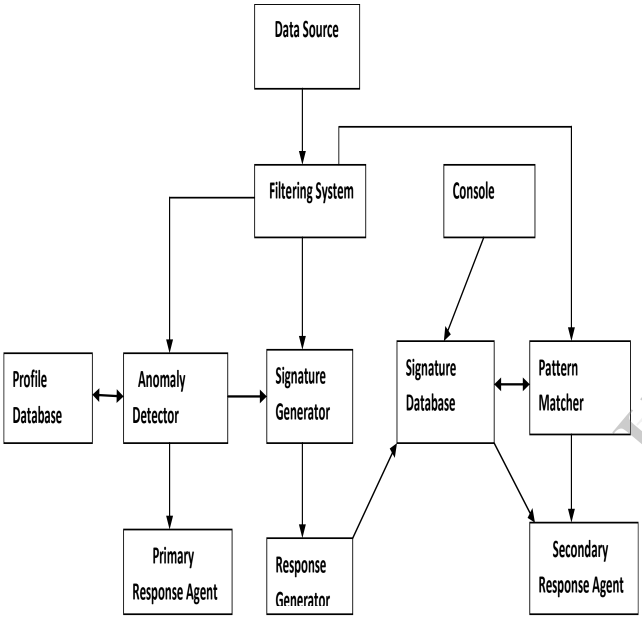


fig1.Architecture Diagram

A)Data Source: The *data source* is responsible for collecting information and supplying a stream of event records to the *filtering system*. The nature of the information collected may vary according to the monitoring strategies adopted3: *host-based*, *network-based*, *application based* or *target-based*. The proposed IDS model is applicable to any of these strategies.

B)Filtering System: The *filtering system* provides audit reduction in order to identify and remove

Relevant information. After filtering, the information stream is passed to the detection, when required, to the *signature generator*.

C)Anomaly Detection System: The *Anomaly detection system* involves a process of establishing profiles of normal behavior. Comparing actual behavior to those profiles and flagging deviations from normal. The components of the anomaly detection system are described as follows:

-Profile database: The *profile database* is responsible for storing the profiles that describes the behavior of the computer system.

− *Anomaly Detector*: The *anomaly detector* receives the event stream from the *filtering system* and verifies if it represents anomalous behavior. In order to do that, it compares the information received with the set of previously established profiles stored in the *profile database*. The *anomaly detector* activates the *primary response agent* and feeds the *signature generator* with the information detected as abnormal.

− *Primary Response Agent:* Once activated, it initiates a series of contention measures to slow down or even block a probable attack. The main purpose of these primary response measures is to minimize damage until a specific and efficient response can be executed. Some examples of such primary responses are file system protection and alarms of intrusive activities.

D)Signature Generator: It is assumed that the anomaly detection system may use a different monitoring strategy from the one adopted by the misuse detection system to be anomalous into a signature that specifically identifies the attack related to that abnormal behavior. It is responsible for this convert ion of anomalous information into a signature of the attack. After the generation of the signature, the *signature generator* activates the *response generator*.

E)Response Generator: The *response generator* receives the signature of the attack and elaborates a set of countermeasures specific to that attack. Both signature and response produced are delivered to the *signature database*.

*F)Misuse Detection System:*Misuse intrusion detection comprehends the search for activity patterns that match a known attack or other violation of security policy. The components of the misuse detection system are described as follows.

− Signature Database

It is responsible for storing the signatures of attacks, relating them to the respective response measures. The signatures are used by the *pattern matcher*, while the countermeasures are consulted by the *secondary response agent*. In this way, the proposed IDS can specifically detect and respond to each manifestation of a known attack in the system.

− Pattern Matcher: It receives the event stream from *filtering system* and matches it with the patterns stored in the *signature database*. The detection is conducted in real time and uses an approach based on state transition:

− Secondary Response Agent: Once activated, the *secondary response agent* receives the pattern that was matched and queries the *signature database* for the specific countermeasures related to that pattern. So the *secondary response agent* executes the countermeasures.

V. PROPOSED SCHEME:

The intrusion detection application concerns how fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, the intruder can be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and may be even unaffordable for a large area. In fact, it is not necessary to deploy so many sensors to cover the entire WSN area in many applications, since a network with small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance. In this case, the application can specify a required intrusion distance within which the intruder should be detected.

VI. APPROACHES

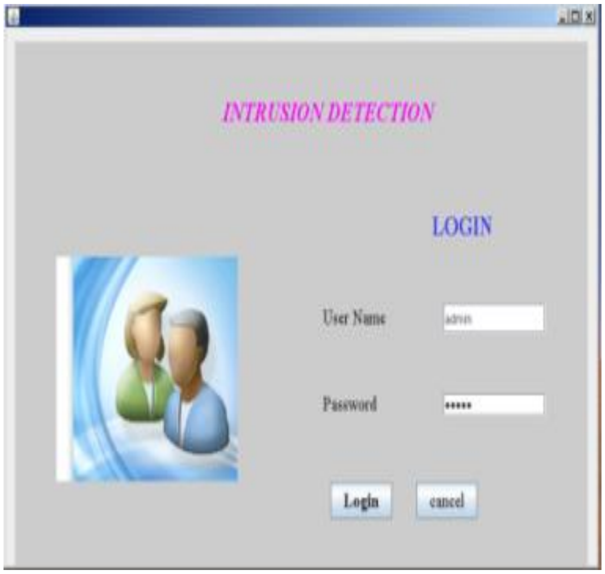
A.CLUSTERING ALGORITHM BASED APPROACH: Loon et al. developed an intrusion detection scheme for routing attacks that uses a fixed-width clustering algorithm to build a model of normal behavior. Note that here we refer to clustering algorithm as unsupervised learning algorithms, not cluster-based network structure. In the training stage, a fixed-width clustering algorithm is used to build a set of clusters in the feature space. Clusters that contain less training traffic samples than a specific threshold are identified as anomalous. During the testing stage, each traffic sample is compared to the cluster set to determine whether it is anomalous The IDS has two stages: profile learning and anomaly detection. In the anomaly detection phase, a pattern matching technique is used to detect any unknown subsequences of packet events **Benefits**: The results show that the algorithm is able to detect. The algorithm is adaptive in the sense that each node might have a different detection model.

B. CENTRALISED APPROACH: A centralized, active anomaly detection system called ANDES was proposed by Gupta et al. In this IDS the detection agent is located in the base station, collecting application data, management information (e.g. node’s ID, hops towards the sink, total transmitted packets, total number of failures to route a packet), and node status information (e.g. normal, unavailable, duplicated and abnormal state), amongst others. All this information can then be combined and analyzed in order to identify possible anomalies. ***Benefits****:* This system was implemented in TinyOS on Tmote sky sensor nodes. While the management information might impose a certain overhead as additional management traffic must be acquired.

C.ISOLATION TABLE: Chen et al. proposed an anomaly detection method for three-level hierarchical WSNs (base station - primary cluster heads - secondary cluster heads) based on an isolation table. In this method the isolation table records the anomaly information, and the detection agents use it to isolate nodes from the network. Note that these tables can be generated by all cluster heads), and all tables are forwarded to the base station. As a result, isolation tables can be provided to any node that needs them (e.g. a newly elected cluster head that needs to know the actual state of the network). The applicability of this method was analyzed using the ns-2 simulator.

VII.RESULT AND ANALYSIS:

Login page

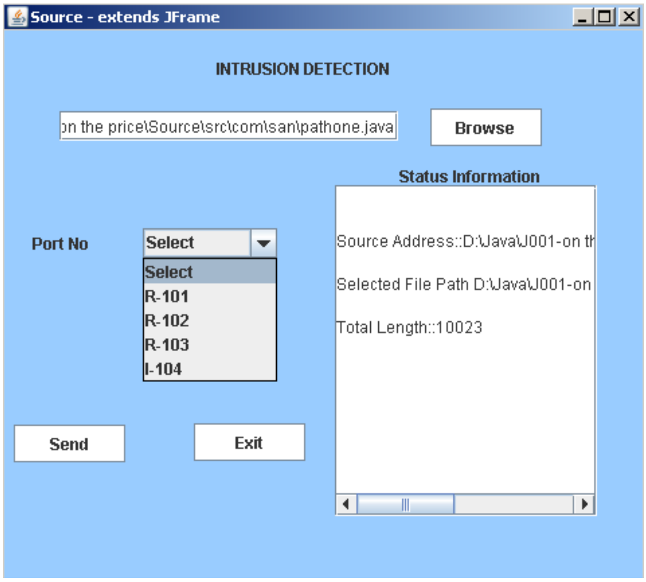


User Name admin

Password •••••

The above screen is the login screen of this project, you will give username as admin and password as admin, after click login, it consider you are authorized user then directly goes to the sender page.

Shows Port number

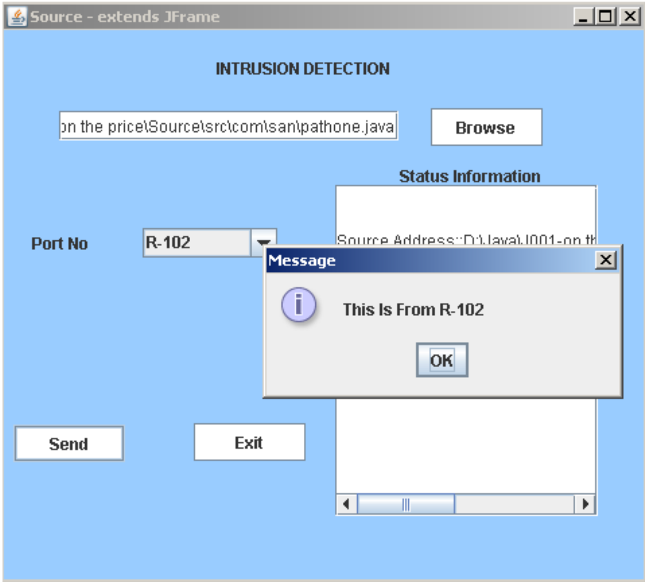


File: on the price\Source\src\com\san\pathone.java

```
Source Address::D:\Java\J001-on th
Selected File Path D:\Java\J001-on
Total Length::10023
```

The above screen is the source node ,it shows the port number available in this project

Using Port number to Send



File: on the price\Source\src\com\san\pathone.java

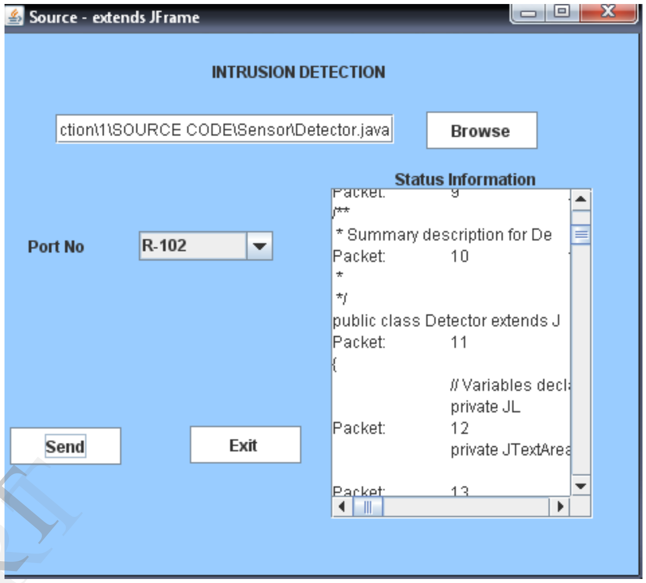
Port No: R-102

```
Source Address::D:\Java\J001-on th
```

This Is From R-102

This screen is the source node,the sender will upload the file using browse button ,then select the port number any one in the list box(R-101,R-102,R-103)after clicking the send button it shows the message dialog box ,which port number its come from.

Packet Splitting:



File: ction\1\SOURCE CODE\Sensor\Detector.java

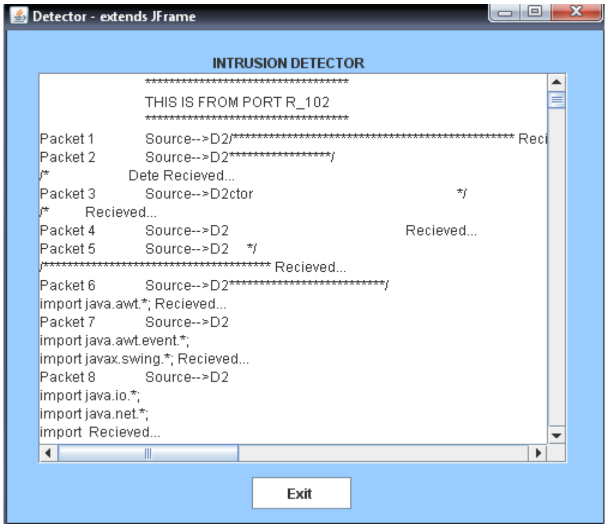
Port No: R-102

```
Packet:            9
/**
 * Summary description for De
Packet:            10
 *
 */
public class Detector extends J
Packet:            11
{
                   // Variables decl
                   private JL
Packet:            12
                   private JTextArea

Packet:            13
```

This screen is the packet splitting .after clicking send button, ur uploaded text files is converted into packet format show in text area box after that it automatically send to Detector

Detector



```
               ***********************************
               THIS IS FROM PORT R_102
               ***********************************
Packet 1       Source-->D2/************************************************ Reci
Packet 2       Source-->D2*****************/
/*           Dete Recieved...
Packet 3       Source-->D2ctor                                  */
/*      Recieved...
Packet 4       Source-->D2                               Recieved...
Packet 5       Source-->D2    */
/*************************************** Recieved...
Packet 6       Source-->D2***************************/
import java.awt.*; Recieved...
Packet 7       Source-->D2
import java.awt.event.*;
import javax.swing.*; Recieved...
Packet 8       Source-->D2
import java.io.*;
import java.net.*;
import  Recieved...
```

This screen is the detector, this detector checks authorized user or not in the available network ,if it is authorized its send to receiver, or it discard the packets

V. CONCLUSIONS

In this work, we have provided a detailed and comprehensive study on IDSs in wireless sensor networks, classifying them according to their underlying mechanisms. In addition, we have briefly introduced the existing security attacks in WSNs and their respective countermeasures. Furthermore, we have provided a critical analysis of the IDS mechanisms with respect to network structure, highlighting various vital areas that are currently underdeveloped. Based on our observations and findings we can conclude that, while the field of IDS for WSN has advanced significantly in these last years, there are still various research areas (e.g. IDS architectures, balance between accuracy and consumption of resources, novel scenarios, better integration of underlying mechanisms) that need to be further developed. We hope that our results will be beneficial for both beginners and active researchers in this area.

REFERENCES

[1] Y. Zhou, Y. Fang, and Y. Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Commun. Surveys Tutorials, vol. 10, no. 3, pp. 6-28, 2008.

[2] A.-S. K. Pathan, H.-W. Lee, and C.S. Hong, Security in Wireless Sensor Networks: Issues and Challenges, in 8th International Conference on Advanced Communication Technology (IEEE ICACT 2006), Volume II, 20-22 February, Phoenix Park, Korea, 2006, pp. 1043-1048.

[3] I. Onat and A. Miri, An Intrusion Detection System for Wireless Sensor Networks, Wireless and Mobile Computing, Networking And Communications, vol. 3, 2005, pp. 253-259.

[4] R. Roman, J. Zhou, and J. Lopez, Applying Intrusion Detection Systems to Wireless Sensor Networks, in Consumer Communications and Networking Conference, 2006, pp. 640-644.

[5] CE. Loo, MY. Ng, C. Leckie, and M. Palaniswami, Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, vol. 2, pp. 313-332, 2006.

[6] Y. Wang, G. Attebury, and B. Ramamurthy, A Survey of Security Issues in Wireless Sensor Networks, IEEE Commun. Surveys Tutorials, vol.8, pp. 2-23, 2006.

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

[8] L. Mostarda, and A. Navarra, Distributed Intrusion Detection Systems for Enhancing Security in Mobile Wireless Sensor Networks, International Journal of Distributed Sensor Networks, vol. 4, no. 2, pp. 83-109,
2008.

[9] Y. Wang, X. Wang, B. Xie, D. Wang, and P. Agrawal, Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks, IEEE Trans. Mobile Computing, vol. 8, no. 6, pp. 698-711, 2008.

[10] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A Survey on Sensor Networks, IEEE Commun. Mag., vol. 40, no. 8, pp. 102-114,August 2002.

[11] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks, LNCS,vol. 4837, pp. 150-161, 2008.

[12] L. Guorui, H. Jingsha, and F. Yingfang, Group-based Intrusion Detection System in Wireless Sensor Networks, Computer Communications, vol. 32, no. 18, pp. 4324-4332, 2008.

[13] I. Krontiris, T. Dimitriou, and T. Giannetsos, LIDeA: a Distributed Lightweight Intrusion Detection Architecture for Sensor Networks, in 4th International Conference on Security and Privacy in Communication Networks, Istanbul, Turkey, 2008.

[14] A.P.R. da Silva, M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro, L.B.Ruiz, and H.C. Wong, Decentralized Intrusion Detection in Wireless Sensor Networks, in 1st ACM International Workshop on Quality of service and security in wireless and mobile networks, Montreal, Quebec, Canada, October 2005.

[15] I. Krontiris, T. Dimitriou, and F.C. Freiling, Towards Intrusion Detection in Wireless Sensor Networks, in 13th European Wireless Conference, Paris, France, 2007.