Problems and Challenges in Wireless Network Intrusion Detection

Ms. Ami Desai, Ms. Hiral Prajapati, Mr. Dharmendra Bhatti

ABSTRACT

Wireless ad hoc sensor network becomes popular in civil and military jobs. But security is one of the significant challenges for sensor network because of their deployment in open and unprotected environment. As cryptographic mechanism is not enough to protect sensor network from external attacks, intrusion detection system needs to be introduced. Though intrusion prevention mechanism is one of the major and efficient methods against attacks, but there might be some attacks for which prevention method is not known. Besides preventing the system from some known attacks, intrusion detection system gather necessary information related to attack technique and help in the development of intrusion prevention system.

In addition to reviewing the present attacks available in wireless sensor network this paper examine the hierarchical architectural design based intrusion detection system that fits the current demands and restrictions of wireless ad hoc sensor network. In this paper, intrusion detection system architecture clustering mechanism is to build a four level hierarchical network which enhances network scalability to large geographical area and use both anomaly and misuse detection techniques for intrusion detection. In this proposed Intrusion Detection System architecture, we propose a new approach of an Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks.

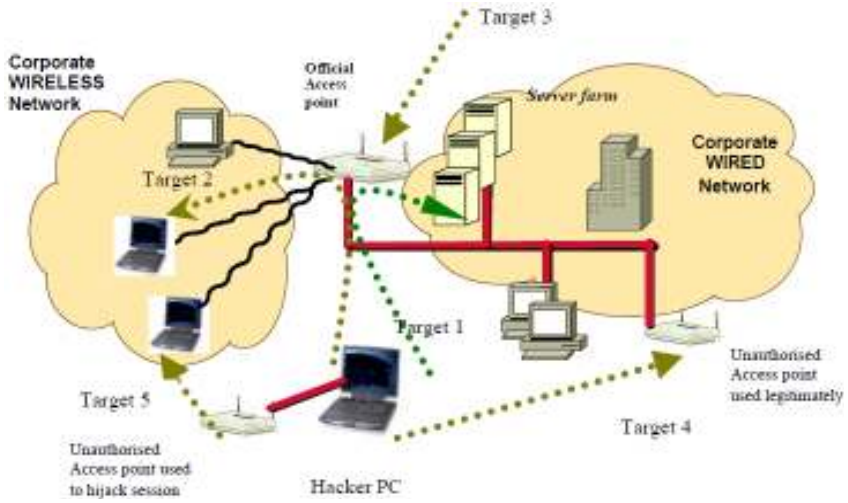
Keyword: WSN, IDS, Hierarchical Design, Security, Sensor Node, Cluster Node, Regional Node, Base Station

1. INTRODUCTION

An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of a certain system. The task of Intrusion Detection Systems (IDS) is to monitor computer networks and systems, detecting possible intrusions in the network, and alerting users after intrusions had been detected, reconfiguring the network if this is possible[1].A wireless IDS perform this task exclusively for the wireless network.

Although there have been some recent developments in the area of IDS systems for wireless networks, there is no previous work reported in the literature about IDS architectures for wireless sensor networks. In this paper we propose a hierarchical architectural design based intrusion detection system that fits the current demands and restrictions of wireless ad hoc sensor network. In this paper, intrusion detection system architecture followed clustering mechanism to build a four level hierarchical network which enhances network scalability to large geographical area and use both anomaly and misuse detection techniques

for intrusion detection. Here, policy based detection mechanism as well as intrusion response together with GSM cell concept for intrusion detection architecture is used.



[Figure 1: The Wireless Network - What is attacked]

The diagram above shows the various elements of the wireless network and how these can be attacked.

2. EXISTING CHALLENGES

Existing intrusion detection systems are not adequate to protect Wireless Sensor Network from Inside and Outside attackers. None of them are complete. E.g. most of the approaches offer clustering techniques without mentioning how they will be formed and how will they behave with rest of the system. Most of the existing IDSs deal with wired architecture except their wireless counterpart. The architecture of WSN is even more sophisticated than ad hoc wireless architecture. So, IDS is needed with capability of detecting inside and outside, known and unknown attacks with low false alarm rate. Existing IDS architecture that are specifically designed for sensor networks are suffering from lack of resources e.g. high processing power, huge storage capabilities, unlimited battery backup etc.

3. WIRELESS SENSOR NETWORK – OVERVIEW

As per the NIST (National Institute of Standards and Technology) "*a wireless ad hoc sensor network consists of a number of sensors spread across a geographical area"* [4].The term *sensor network* refers to a system which is a combination of sensors and actuators with some general purpose computing elements. A sensor

network can have hundreds or even thousands of sensors; mobile or fixed locations; deployed to control or monitor [3].A wireless sensor network comprises of sensor nodes to sense data from their environment, and passes it on to a centralized controlling and data collecting identity called *base station*. Typically, base stations are powerful devices with a large storage capacity to store incoming data. They generally provide gateway functionality to another network, or an access point for human interface [2]. A base station may have an unlimited power supply and high bandwidth links for communicating with other base stations. In contrast, wireless sensors nodes are constrained to use low power, low bandwidth, and short range links.

4. SECURITY THREATS AND ISSUES

Many types of security issues and threats that are considered for wireless ad hoc network can be applied for WSN. But the security mechanism used for wireless ad hoc networks cannot be deployed directly for WSNs because of their architectural inequality.

1. In ad hoc network, every node is usually held and managed by a human user. Whereas in sensor network, all the nodes are independent and communication is controlled by base station.
2. Computing resources and batteries are more constrained in sensor nodes than in ad hoc nodes.
3. The purpose of sensor networks is very specific e.g. measuring the physical information (such as temperature, sound etc.).
4. Node density in sensor networks is higher than in ad hoc networks [5]. Architectural aspect of WSN makes the security mechanism more prosperous as the base station could be used intelligently.

As per the basic needs of security attacks in WSN can be categorized:

- DoS, DDoS, attacks which affect network *availability*
- Eavesdropping, sniffing which can threaten confidentiality
- Man-in-the-middle attacks which can affect packet integrity
- Signal jamming which affect *communication*

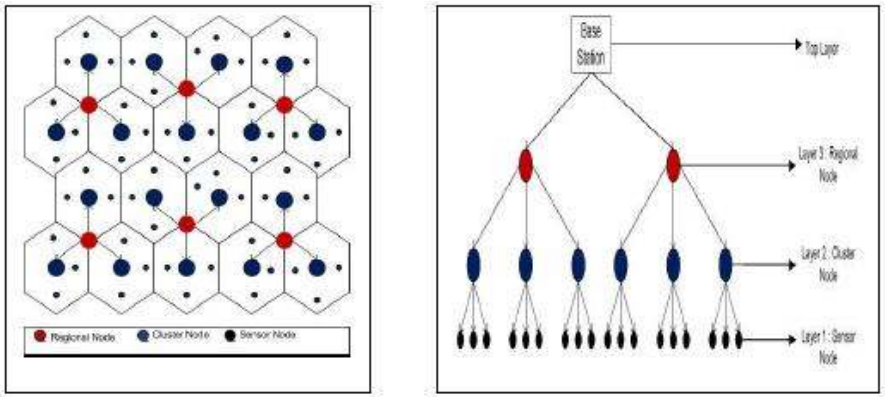
There has been much research work that has been done in the area of significant security problems. Here some of the existing well-known threats are as follows:

Attacks	**Brief Description**
Attack on information in transit	Information that is to be sent can be modified, altered, replayed, spoofed, or vanished by attacker.
Hello flood	Attacker with high radio range sends more Hello packet to announce themselves to large number of nodes in the large network persuading themselves as neighbor.
Sybil attack	Fake multiple identities to attack on data integrity and accessibility.
Wormhole attack	Transmit information between two WSN nodes in secret.
Network partition attack	Threats to accessibility though there is a path between the nodes.
Black Hole Attack	The attacker absorbs all the messages.
Sink Hole Attack	Similar to black hole. Exception: the attacker advertises wrong routing information
Selective Forwarding	The attacker forwards messages on the basis of some Preselected Criterion
Simple Broadcast Flooding	The attacker floods the network with broadcast Messages.
Simple Target Flooding	The attacker tries to flood through some specific nodes.
False Identity Broadcast Flooding	Similar to simple broadcast flooding, except the attacker deceives with wrong source ID.
False Identity Target Flooding	Similar to simple target flooding, except the attacker deceives with wrong source ID.
Misdirection Attack	The attacker misdirects the incoming packets to a distant node.

Table 1: Threats and Attacks in WSN

5. MODEL FOR IDS

In this paper, we propose a new model for the IDS which is concentrates on saving the power of the sensor nodes by distributing the responsibility of the intrusion detection to three layers nodes with the help of policy base network management system. This model uses hierarchical overlay design (HOD). Here we divide each area of the sensor nodes into hexagonal region[11]. Sensor nodes in each of the hexagonal area are monitored by a cluster node. Each cluster node is then monitored by the regional node. Again the Regional nodes will be controlled and monitored be the Base Station.



[Figure 2: Hierarchical Overlay Design]

This HOD based IDS combines' two approaches of intrusion detection mechanisms (Signature and anomaly) together to fight against existing threats. Signatures of well-known attacks are propagated from the base station to the leaf level node for detection. Signature repository at each layer is updated as new forms of attacks are found in the system[13]. As intermediate agents are activated with predefined rules of system behavior, anomaly detection can take part from the deviated behavior of predefined specification. Thus proposed IDS can identify known as well as unknown attacks.

Detection Entities

There are four types of detection entity and these are as follows:

1. Sensor Nodes

2. Cluster Nodes

3. Regional Nodes

4. Base Station

1. **Sensor Nodes:**

Sensor Nodes have two types of functionality: Sensing and Routing. Each of the sensor nodes will sense the environment and exchange data in between sensor nodes and cluster node[15]. As sensor nodes have much resource constraints, in this model, there is no IDS module installed in the leaf level sensor nodes.

2. **Cluster Nodes:**

Cluster Node plays as a monitor node for the sensor nodes. One cluster node is assigned for each of the hexagonal area. It will receive the data from sensor nodes, analyze and aggregate the information and send it to regional node. It is more powerful than sensor nodes and has intrusion detection capability built into it.

3. **Regional Nodes:**

Regional Node will monitor and receive the data from neighboring cluster heads and send the combined alarm to the upper layer base station. It is also a monitor node like the cluster nodes with all the IDS functionalities. It makes the sensor network more scalable. If thousands of sensor nodes are available at the leaf level then the whole area will be split into several regions.

4. **Base Station:**

Base Station is the topmost part of architecture empowered with human support. It will receive the information from Regional nodes and distribute the information to the users based on their demand.

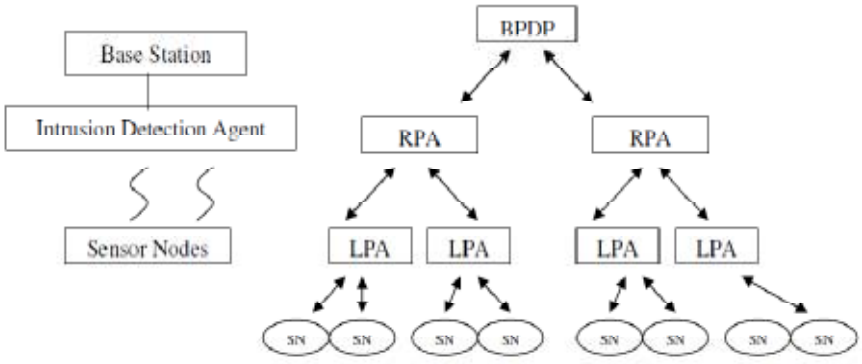
Policy based IDS

Policy implies predefined action pattern that is repeated by an entity whenever certain conditions occur [11]. The architectural components of policy framework include a Policy Enforcement Point (PEP), Policy Decision Point (PDP), and a Policy repository. The policy rules stored in Policy repository are used by PDP to define rules or to show results. PDP translates or interprets the available data to a device-dependent format and configures the relevant PEPs. The PEP executes the logical entities that are decided by PDP [10]. These capabilities provide powerful functions to configure the network as well as to re-configure the system as necessary to response to network conditions with automation. In a large WSN where Hierarchical Network Management is followed can be realized by policy mechanism to achieve survivability, scalability and autonomy simultaneously. So in case of failure the system enables one component to take over the management role of another component. One of the major architectural advantages of hierarchical structure is any node can take

over the functionality of another node dynamically to ensure survivability. A flexible agent structure ensures dynamic insertion of new management functionality.

Hierarchical network management integrates the advantage of two (Central and Distributed) management models [12] and uses intermediate nodes (Regional and Cluster) to distribute the detection tasks. Each intermediate manager has its own domain called Regional or Cluster agent which collects and processed information from its domain and passes the required information to the upper layer manager for further steps. All the intermediate nodes are also used to distribute command/data/message from the upper layer manager to nodes within its domain. It should be noted that there is no direct communication between the intermediate members. Except the leaf level sensor nodes all the nodes in the higher level are configured with higher energy and storage.

To achieve a policy-based management for IDS the proposed architecture features several components that evaluate policies: a Base Policy decision Point (BPDP), a number of Policy decision modules (PDMs) and Policy Enforcement Point (PEP).



BPDP: Base Policy Decision Point
RPA: Regional Policy Agent
LPA: Local Policy Agent
SN: Sensor Node

[Figure 3: Hierarchical Architecture of IDS Policy Management]

Base Policy Decision Point (BPDP):

Base Policy Decision Point (BPDP) is the controlling component of the architecture. It implements policies or intrusion rules generated by the Intrusion Detection Tool (IDT) from receiving events, evaluating anomaly conditions and applying new rules, algorithms, threshold values etc. IDT supports creation, deletion, modification, and examination of the agent's configurations and

policies. It can add new entities e.g. new signature of intrusion, modify or delete existing entities in RPA and LPA.

Policy Decision Modules (PDMs):

Policy Decision Modules (PDMs) are components that implement sophisticated algorithms in relevant domains. LPAs and RPAs act as PDMs. LPA manages the sensor nodes which is more powerful than sensor nodes. LPAs perform local policy-controlled configuration, filtering, monitoring, and reporting which reduces management bandwidth and computational overhead from leaf level sensor nodes to improve network performance and intrusion detection efficiency. An RPA can manage multiple LPAs. At the peak BPDP manages and controls all the RPAs.

Policy Enforcement Points (PEP):

Policy Enforcement Points (PEP) are low level Sensor Nodes. Policies are disseminated from the BPDP to RPA to LPA as they are propagated from PDP to LPA. Policy agents described above helps IDS by reacting to network status changes globally or locally. It helps the network to be reconfigured automatically to deal with fault and Performance degradation according to intrusion response.

Selection of IDS node

Activating every node as IDS, wastes energy. So minimization of number of nodes to run intrusion detection is necessary. In [13] three strategies are mentioned involving selection of Intrusion detection node.

Core defense selects IDS node around a center point of a subset of network. It is assumed that no intruder break into the central station in any cluster. This type of model defends from the most inner part then retaliates to the outer area.

Boundary defense selects node along the boundary perimeter of the cluster. It provides defense on intruder attack from breaking into the cluster from outside area of the network.

Distributed defense has an agent node selection algorithm which follows voting algorithm from [16] in this model. Node selection procedure follows tree hierarchy.

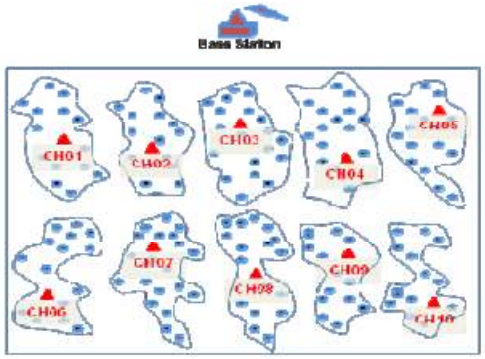
The model follows **Core Defense strategy** where cluster-head is the center point to defend intruders. In core defense strategy ratio of alerted nodes and the total number of nodes in the network drops, this makes energy consumption very low which make it more economical in their use of energy as it shows least number

of broadcast message in case of attack. It has strong defense in inner network. Here IDS needs to wait for intruder to reach the core area which is one of the drawbacks of this strategy as nodes can be captured without notice.

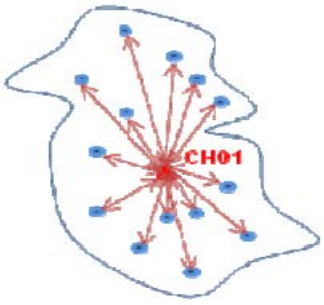
6. PROPOSED INTRUSION DETECTION BASED SECURITY SOLUTION

The main emphasis of this approach is to detect and prevent the intruder in the sensor network by implementing the MAC address based intruder tracking system.

The layout of the wireless sensor network is as follows:



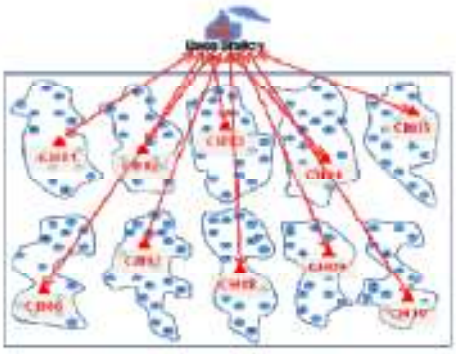
[Figure 7: Layout of Wireless Sensor Network]



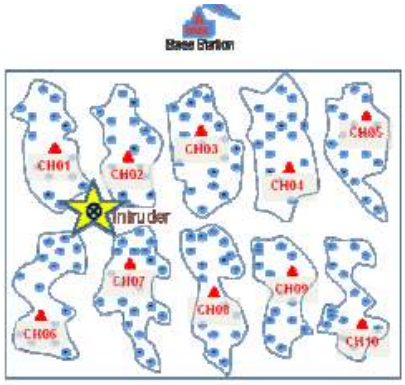
[Figure 8: Data Communication between Nodes and its CH]

As shown in above first figure, let us assume a wireless sensor network consisting of 10 Cluster heads (CH01 to CH10) with their node forming the clusters. Nodes send data to their respective cluster heads (CHs) within each cluster. As shown in second fig., the CH collects data from each node, compresses the data and transmits it to the Base Station (BS). CHs keep track of each node and send periodic status information to the BS. BS exchanges data from nodes through the cluster heads. It keeps track of the healthiness of all the nodes in each cluster by checking the MAC address information sent by each CH.

As illustrated in below figure, any change in cluster architecture because of change in CH is controlled and monitored by the BS. Intruder tries to communicate with one of the nearest available node and become a part of this network as depicted in Figure:



[Fig. 9: Data Communication between CHs & BH]



[Fig. 10: Intruder introduced in the network]

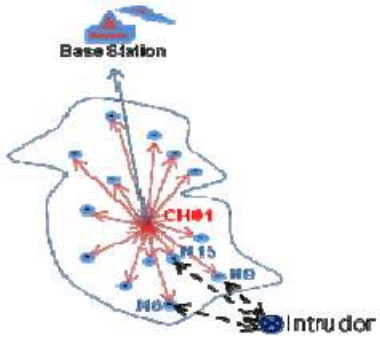
Possible Intrusion:

The intruder can try to merge into the network system in the following two ways:

1. Intruder tries to bond with one of the nodes in a cluster
2. Intruder tries to bond with a Cluster Head of a cluster

7. INTRUDER TRIES TO BOND WITH ONE OF THE NODES IN A CLUSTER

Assume that the intruder identifies N15, N9 and N6 in the first cluster as the nearest possible nodes. As shown in Figure, the intruder tries to communicate with one of the nodes (N15, N9 or N6) with hidden MAC address in listen mode only.

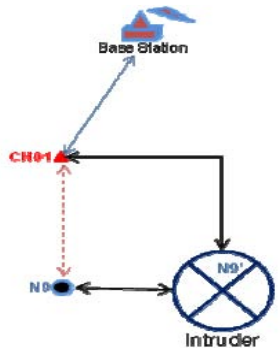


[Figure 11: Intruder trying to communicate with its nearest node]

It successfully bonds with node N9 in listen mode keeping its identity hidden. The Intruder has the capability of interpreting the packets being sent and received by node N9.

The MAC address of the node N9 and the MAC address of the CH can be deciphered by the intruder which shall help it to merge into the network.

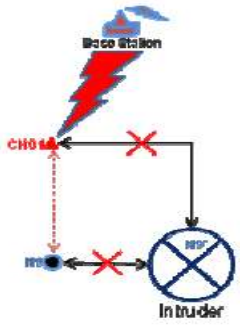
In Figure, with the information of the MAC address of the node N9 and CH, the intruder tries to create a duplicate node N9' and duplicate CH as CH01'. The basic intention is to route the information through intruder and shutdown the node N9. The moment intruder tries to route data through the duplicate identity; the CH identifies un-known MAC address of the intruder. This information is passed immediately to the BS to take the necessary corrective action, as shown in the following figure.



[Figure 12: Un-known MAC address identified by Cluster Head]

As a corrective action the BS broadcasts an alarm to all the CHs regarding identity of the intruder. The Cluster Head CH01 is instructed to block the

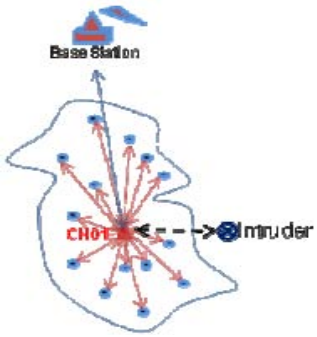
receiving and sending of data to ensure that the intruder can no longer infect the functioning of the wireless sensor network. This phenomenon is illustrated in following figure.



[Figure 13: Base station identifies intruder and broadcasts information to all CHs]

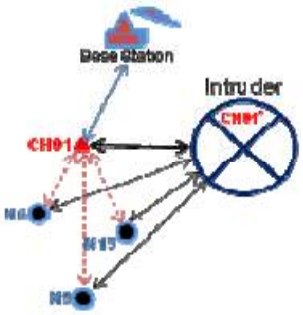
8. INTRUDER TRIES TO BOND WITH A CLUSTER HEAD OF A CLUSTER

Assume that the intruder identifies Cluster Head CH01 as the nearest possible node. In this figure, the intruder tries to communicate with CH01 with hidden MAC address in listen mode only.

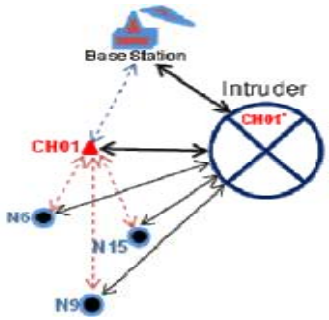


[Figure 14: Intruder trying to communicate with Cluster Head CH01]

With the information of the MAC address of CH01 the intruder tries to create a duplicate Cluster Head CH01. The basic intention is to route the information through intruder and shutdown the Cluster Head CH01. The moment intruder tries to route data through the duplicate identity; CH identifies un-known MAC address of the intruder. This information is passed immediately to the Base Station to take the necessary corrective action, as shown in below Fig. :

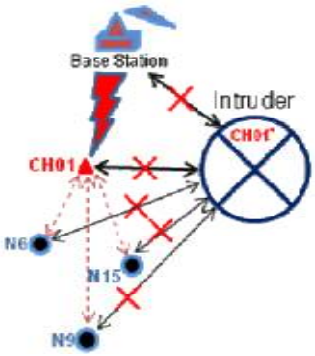


[Fig. 15: Intruder tries to duplicate identified node CH01]



[Fig. 16: Un-known MAC address base station]

As a corrective action the BS broadcasts an alarm to all the CHs regarding the identity of the intruder. As shown in Fig. below, the Cluster Head CH01 is instructed to block the receiving and sending of data to ensure that the intruder can no longer infect the functioning of the wireless sensor network.



[Figure 17: Base station identifies intruder and broadcasts information to all CHs]

9. CONCLUSION

In this paper, we had provides the security solution for the cluster nodes using Cluster-Based Wireless Sensor Networks. Here, MAC address based intruder tracking system is used for Cluster-Based Wireless Sensor Networks. This proposed system implements the base station based detection and very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by the security system can prevent many security problems like slow down the network, passes the fake data and many more. By designing the security system in which the Base Station

examines and track the security of the wireless network, high security can be achieved.

10. REFERENCES

1. R. Bace. *Intrusion Detection*. MacMillan Technical Publishing, 2000.
2. Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30. January, 2008.
3. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May 11, 2003).
4. National Institute of Standards and Technology, "Wireless ad hoc sensor networks", web: http://w3.antd.nist.gov/wahn_ssn.shtml, retrieved 12th January, 2008.
5. Rodrigo Roman, Jianying Zhou, Javier Lopez, "Applying Intrusion Detection Systems to wireless sensor networks ", Consumer Communications and Networking Conference, 2006. CCNC2006. 3rd IEEE, 8-10 Jan. 2006 Volume: 1, On page(s): 640- 644 ISBN: 1-4244-0085-6
6. FZhang, Y. and Lee W "Intrusion detection in Wireless Ad hoc Networks", The 6th annual international conference on Mobile computing and networking, Boston MA, Aug 2000. PP:275-283
7. . P.Bruth and C. Ko, "Challenges in Intrusion detection for wireless ad hoc networks" in Application and the Internet Workshop =s, 2003 proceedings,2003 Symposium on, PP.368-373,2003.
8. Article on "An Introduction to Intrusion Detection Systems" by Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC
9. Anderson, Ross (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. pp. 387–388. ISBN 9780471389224.
10. R. Chadha, G. Lapiotis, S. Wright, "Policy-Based Networking", IEEE Network special issue, March/April 2002, Vol. 16 No. 2, guest editors.
11. LinnyerBeatrysRuizıJose Marcos Nogueira and Antonio A. F. Loureiro. MANNA: A Management Architecture for Wireless Sensor Networks IEEE Communications Magazine, 2003.2b:
12. http://w3.antd.nist.gov/wahn_ssn.shtml, retrieved 1[68]. Zhou Ying, Xiao Debao, "Mobile agent based Policy management for wireless sensor network", ISBN: 0-7803-9335-X/05, 2005 IEEE.
13. W. Chen, N. Jain and S. Singh, "ANMP: Ad hoc Network Management protocol", IEEE Journal on Selected Areas in Communications17 (8) (August 1999) 1506-1531.

14. Piya Techateerawat, Andrew Jennings, "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks", Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06) 0-7695-2749-3/06
15. Bharat Bhargava, Weichao Wang. Visualization of Wormholes in Sensor Networks. New York, NY, USA: ACM Press, 2004.

AUTHOR'S PROFILE

Ms. Ami Desai, MCA (Pursuing) is Student of Shrimad Rajchandra Institute of Management and Computer Application, affiliated to Gujarat Technological University, Ahmedabad. She is "IBM Tivoli Directory Server V6.1" and "IBM DB2 9 Fundamental" certified. She also got the 1st Rank during Graduation. She has written one Article. She is Active Member of Computer Society of India.

Ms. Hiral Prajapati, MCA (Pursuing) is Student of Shrimad Rajchandra Institute of Management and Computer Application, affiliated to Gujarat Technological University, Ahmedabad. She is "IBM Tivoli Directory Server V6.1" and "IBM DB2 9 Fundamental" certified. She also got the 1st Rank during Graduation. She has written one Article. She is Active Member of Computer Society of India.

Prof. Dharmendra G. Bhatti is an Associate Professor of MCA program at Shrimad Rajchandra Institute of Management and Computer Application, Bardoli, Gujarat, India. He received his MCA degree from South Gujarat University in the year 2000. His research area includes Network Security, Soft Computing Techniques, and Network Administration. He is having 11 years of experience and pursuing Ph.D. in Intrusion Detection using Soft Computing. He has published 1 research papers in International journal and 2 research papers in National journal. He has presented 7 research papers in National conferences/seminars and attended 9 winter/summer school. He is life member of Computer Society of India and achieved 6 IBM Certifications. He manages wired/wireless network of more than 1000 computers. He also handles windows active directory infrastructure, database servers, web server, proxy server, email service, and software licensing.