Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks

Shio Kumar Singh [1], M P Singh [2], and D K Singh [3]
[1]*Maintenance Engineering Department (Electrical), Tata Steel Limited, Jamshedpur – 831001, Jharkhand, India, shio.singh@tatasteel.com*
[2] *Computer Science and Engineering Department, National Institute of Technology, Patna, Bihar, India, writetomps@gmail.com*
[3] *Electronics and Communication Engineering Department, Birsa Institute of Technology, Sindri, Dhanbad –828123, Jharkhand, India, dksingh_bit@yahoo.com*

Abstract

Wireless sensor network (WSN) is an emerging technology that shows great promise for various applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks, which presents a demand for providing security mechanisms in the network.

In this paper, we propose a new approach of an Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks. In the proposed methodology, an efficient MAC address based intruder tracking system has been developed for early intruder detection and its prevention.

Keywords: *Wireless Sensor Networks (WSNs), Cluster Head (CH), Base Station (BS), Intrusion Detection System (IDS)*

1. Introduction

Security is becoming a major concern for protocol designers of WSN because of the broad security-critical applications of wireless sensor networks (WSNs). To protect a network, there are usually several security requirements, which should be considered in the design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements. In many cases, no matter how carefully we design a security infrastructure for a network, attackers may still find a way to break into it and launch attacks from the inside of the network. If they just keep quiet to eavesdrop on traffic flows, they can stay safe without being detected. If they behave more actively to disrupt the network communications, there will be some anomalies, indicating the existence of malicious intrusion or attacks. An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of the wireless network system. Intrusion detection mechanisms can detect malicious intruders based on those anomalies. Intrusion detection system (IDS) attempts 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], [2]. Usually, the neighbors of a malicious node are the first entities learning those abnormal behaviors. Therefore, it is convenient to let each node monitor its neighbors such that intrusion detection mechanisms can be triggered as soon as possible.

In case of cluster-based hierarchical routing wireless sensor network, network topology depend on communication range of the nodes, location information, distance between the nodes and remaining battery power [3], [4], [5], [6], [7], [8]. An intruder can manipulate these parameters to mount spoofed, altered, or replayed routing information attack and attract the network towards it to create a sinkhole. This sink hole may turn into black hole if it absorbs the data completely. These protocols transmit data in multi-hop so intermediate nodes take the responsibility of data aggregation/fusion and forward data to upper level. An adversary who joins the network in setup phase can selectively forward data to upper level and change the data to lead data integrity attack. Attacker can mount adversary nodes with same id in different place of the network and actively join the network. These nodes generate the false data and disrupt the data communication. Also, in multi-hop hierarchical routing, whenever a node sends data to another node, it expects an acknowledgement from the receiving node. Adversary nodes may take the benefit of this and send false acknowledgement for weak and dead nodes to convince the network as alive.

In this paper, we propose Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks. The paper is organized as follows. Section 2 summarizes the related previous works. Section 3 describes the proposed security system. Section 4 provides summary of corrective actions and security solutions for WSN. Conclusion is given in Section 5.

2. Related Previous Works

Continuous monitoring may be energy consuming, which is not desirable in WSNs. Therefore, a cluster-based detection approach is developed for WSNs in Ref. [12]. In this approach, a network is divided into clusters. Each cluster head monitors its cluster members. All the members in a cluster are further divided into groups and the groups take turns to monitor the cluster head. Not all the sensor nodes keep monitoring, thus reducing the overall network energy cost.

The security protocol proposed in Ref. [10] uses local monitoring, in which a neighbor of both a sender and a receiver can oversee the communication behaviors of the receiver. If the receiver has any abnormal behavior on the received packets, it may be detected. If the number of abnormal behaviors is larger than a threshold, the neighbors of the detected malicious node refuse to receive packets from and send packets to it so that the malicious node is isolated from the network.

In Ref. [11], a reputation-based framework is established, in which each node holds reputations for other nodes. Based on the observations of whether other nodes are cooperative or not, those reputations are updated through an iterative procedure and are used as criteria to decide whether a node is malicious or not.

3. Proposed Intrusion Detection Based Security Solution

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

Basic assumption:

- The Base Station (BS) is located far from the sensors and immobile.
- The BS has the information about the location of each node.
- Assume 100 nodes in the network.

- Nodes in the network are not dynamic while the Cluster Heads (CHs) are being selected

Function of Base Station:

- All nodes are able to send data to BS via Cluster Head.
- Base station has all the information regarding each Cluster (number and MAC address)
- The removal or addition of any node in a Cluster is monitored by the Base Station.
- Poll status of each node is received with MAC address.
- Base station runs task of MAC address tracking, MAC address history and management of database.
- The Base Station has the capability to seize the operation of any node in the network

Function of Cluster Head:

- Cluster Heads keep track of each node and sends periodic status information to the Base Station.
- Cluster heads receives data from its nodes and sends necessary information
- Cluster Heads (CHs) transmits data to Base Station after performing data reception and compression

3.1 Layout of the Wireless Senor Network

As shown in Fig. 1, 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 Fig. 2, 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.

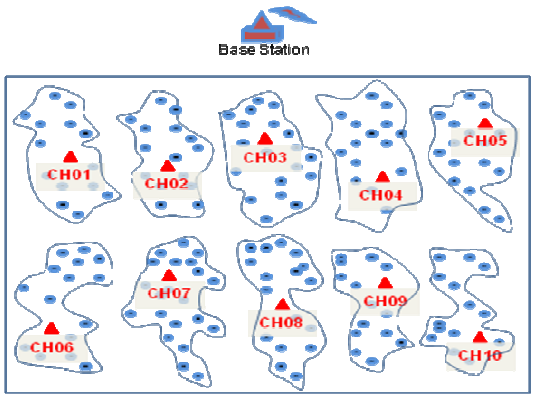


Fig. 1 Layout of Wireless Senor Network

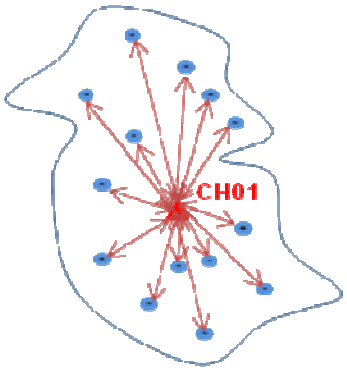


Fig. 2 Data communication between nodes and its CH

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 Fig. 3, any change in cluster architecture due to change in CH or re-organization of the clusters is controlled and monitored by the BS. For example, let us assume that an

intruder comes in this wireless sensor network. It tries to communicate with one of the nearest available node and become a part of this network as depicted in Fig. 4.

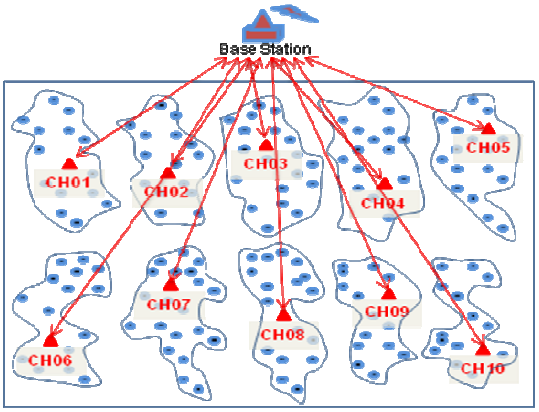


Fig. 3 Data communication between CHs and BS the network

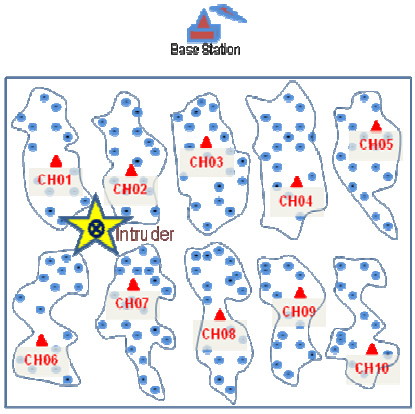


Fig. 4 Intruder introduced in

3.2 Possible Intrusion

The intruder can try to merge into the network system in the following two ways:
Case1 – Intruder tries to bond with one of the nodes in a cluster
Case2 – Intruder tries to bond with a Cluster Head of a cluster

Case 1:

Let us assume that the intruder identifies N15, N9 and N6 in the first cluster as the nearest possible nodes. Shown in Fig. 5, the intruder tries to communicate with one of the nodes (N15, N9 or N6) with hidden MAC address in listen mode only.

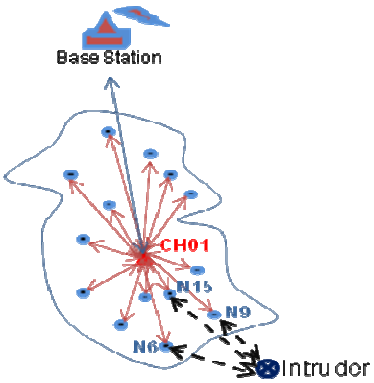


Fig. 5 Intruder trying to communicate communicate with its nearest node

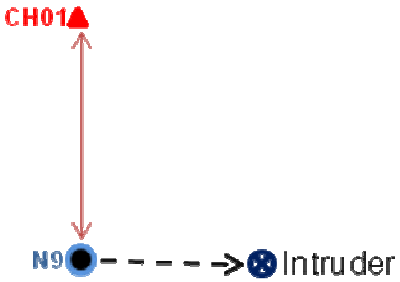


Fig. 6 Intruder trying to with node N9

Finally the intruder identifies node N9 in the first cluster to be the nearest node. As depicted in Fig. 6, it tries to communicate with the node N9 with hidden MAC address in listen mode only. 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, as shown in Fig. 7.

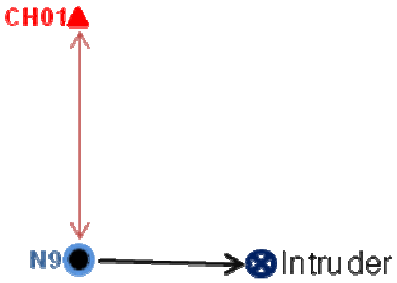


Fig. 7 Intruder establishes communication with N9 in listen mode

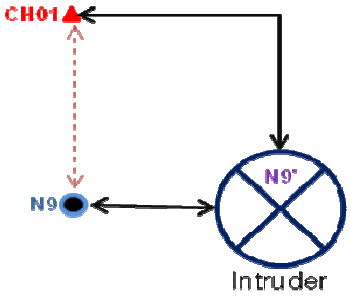


Fig. 8 Intruder tries to create a duplicate node N9'

As illustrated in Fig. 8, 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 Fig. 9.

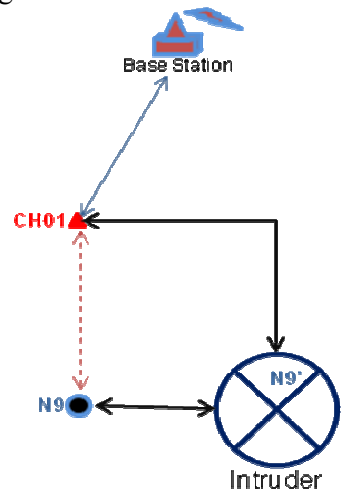


Fig. 9 Un-known MAC address identified by Cluster Head

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 Fig. 10.

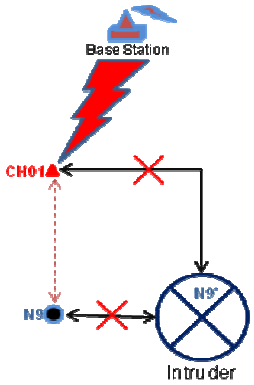
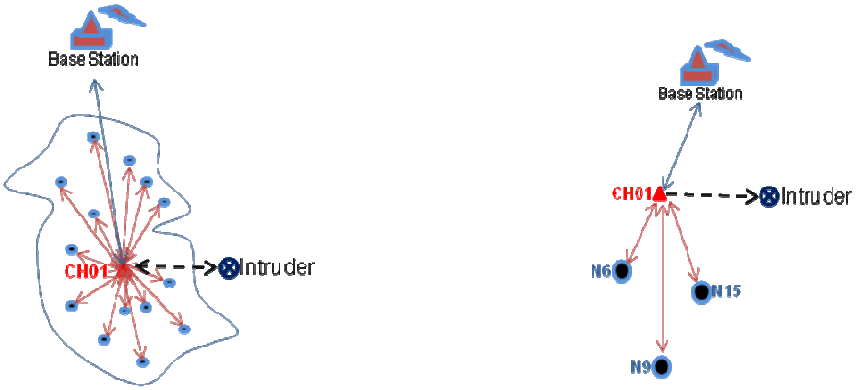


Fig. 10 Base station identifies intruder and broadcasts information to all CHs

Case 2:

Let us assume that the intruder identifies Cluster Head CH01 as the nearest possible node. As illustrated in Fig. 11 (a) and (b), the intruder tries to communicate with CH01 with hidden MAC address in listen mode only.



(a) (b)

Fig. 11 Intruder trying to communicate with Cluster Head CH01

The intruder successfully bonds with Cluster Head CH01 in listen mode keeping its identity hidden. The intruder has the capability of interpreting the packets being sent and received by CH01. As shown in Fig. 12, the MAC address of the CH01 can be deciphered by the intruder which shall help it to merge into the network.

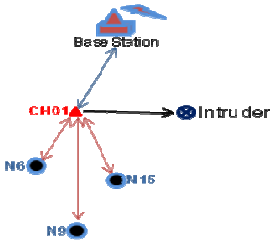


Fig. 12 Intruder establishes communication with create a Cluster Head CH01 in listen mode

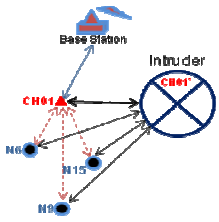


Fig. 13 Intruder tries to duplicate node CH01'

With the information of the MAC address of CH01 the intruder tries to create a duplicate Cluster Head CH01', as shown in Fig. 13. 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 Fig. 14.

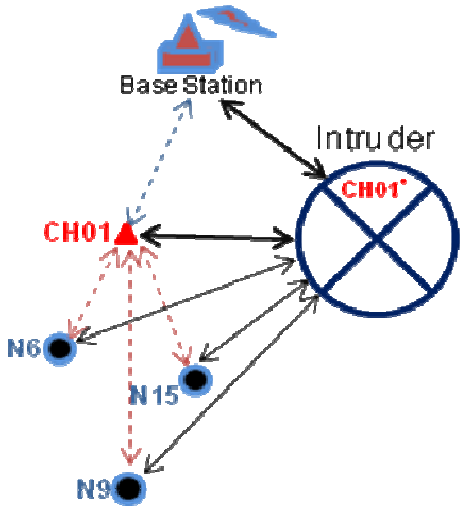


Fig. 14 Un-known MAC address identified by Base Station

As a corrective action the BS broadcasts an alarm to all the CHs regarding the identity of the intruder. As shown in Fig. 15, 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.

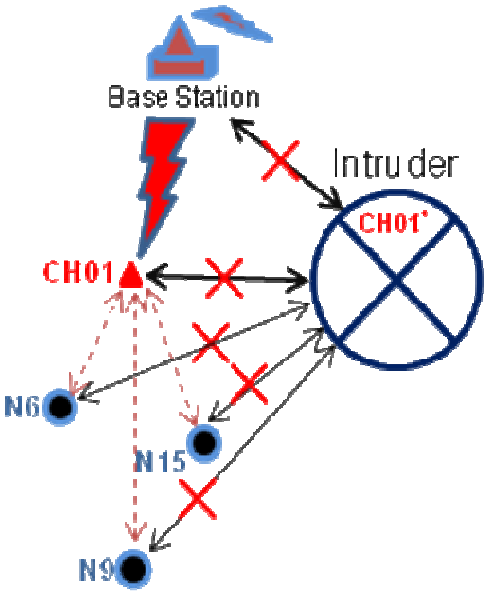


Fig. 15 Base Station identifies intruder and broadcasts information to all CHs

Flow chart in Fig. 16 illustrates the logic of the proposed intrusion detection based security solutions for cluster-based wireless sensor networks.

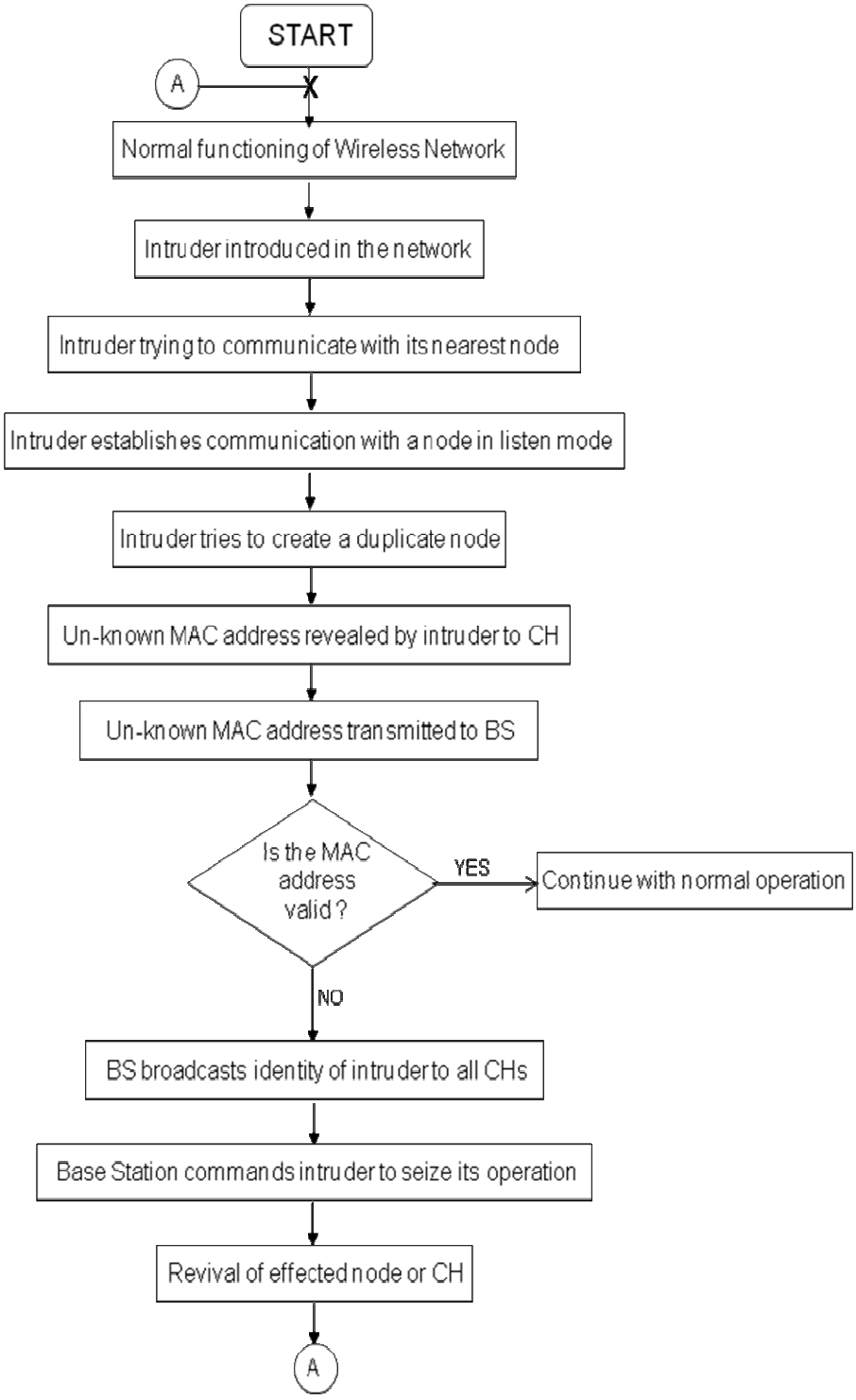


Fig. 16 Intrusion detection for cluster-based wireless sensor network

4. Summary of Corrective Actions and Security Solutions

Case 1 – Intruder tries to bond with one of the nodes in a cluster

- The Base Station collects all the information (location, MAC address, etc) of the intruder. The Base Station issues a command to the intruder to seize its operation (Fig. 10).
- After the intruder has gone down the Cluster Head CH01 revives the affected node N9.
- Hence the functioning of the wireless network is restored.

Case 2 – Intruder tries to bond with a Cluster Head in a cluster

- The Base Station collects all the information (location, MAC address, etc) of the intruder. The Base Station issues a command to the intruder to seize its operation (Fig. 15).
- After the intruder has gone down the BS revives the affected Cluster Head CH01.
- Hence the functioning of the wireless network is restored.

Effect on Energy Efficiency of the Wireless Network

- Same energy is used for sending any message to one or many receivers. Hence, if an intruder is reading the data (in listen node) sent by any node, no additional energy is used by that node.
- When an intruder tries to replace a node or CH, number of send/receive messages are executed. In such case, the send and receive messages are limited as the BS takes immediate action to block the intruder.
- Minimal energy is spent to revive the effected part of wireless network
- Entire security algorithms are handled by the BS. Therefore, no extra load of security detection system is given on the nodes or CHs

Steps for preventing future attacks

- Ensure that the security algorithm / firewall in the Base Station is updated
- An automatic system could be designed which changes the working frequency and channel of the wireless network when an intruder attacks the network
- A more rugged encryption and user authentication system to be deployed

5. Simulation Results

Table 1 shows comparison of various papers published on intrusion detection method for security system of wireless sensor networks [13], [14].

Table : 1 - Comparison of Various Intruder Detection Methods

Parameters	Proposed BS Based Detection	Roman et all [13]	Bhatnagar et all [14]
Method	Base Station detects the intruder using the information sent by the individual Cluster Heads	Few nodes are given rights which act as watchdogs to detect intruders	Nodes detects intruders and passes the information to the nearest dominator which passes the information to the base

			station
Network Overhead	Low (Base Station runs the detection algorithm)	Moderate(Few watchdog nodes runs the detection algorithm)	High (Each node runs the detection algorithm)
Energy Efficiency	High (No extra transmission for intruder detection)	Moderate (Extra transmission by watchdog nodes for intruder detection)	Low (Extra transmission by each nodes for intruder detection)

The result of the proposed system has been further simulated with various assumptions as given below:

Assumptions

- Power consumption assumed for each receive & transmit is 50 nJ/bit
- A 10 KB message is being sent by the intruder to the nodes per mS.
- A 5 KB alarm message is being sent by the node as intruder alarm per mS.
- Power consumed by execution of intruder detection algorithm is 5 nJ/bit

Power consumption per node for Intruder detection system

Power consumption to handle intruder detection and generating alarm ($E_{consume}$) = Power consumption due to receiving of packet from intruder + Power consumption due to processing of intruder detection algorithm + Power consumption due to sending the alarm message

$E_{consume} = (E_{rx} \text{ x Data Packet }) + (E_{process} \text{ x Data Packet}) + (E_{tx} \text{ x Alarm Packet})$
$= (50 \times 10^{-9} \times 10 \times 10^{3}) + (5 \times 10^{-9} \times 10 \times 10^{3}) + (50 \times 10^{-9} \times 5 \times 10^{3})$
$=$ **0.8 mJ / mS**

Case study example

- Let us assume a network comprising of 100 nodes with 10 clusters and 10 Cluster heads
- Let us assume a single intruder in the network system

Case 1 : Proposed Base Station based detection system

Power consumed = $E_{consume}$ x Number of Cluster Heads
= 0.8 x 10 mJ/mS
= 8 mJ/mS

Case 2 : Normal Sensor Node based detection system

Power consumed = $E_{consume}$ x Number of Nodes
= 0.8 x 100 mJ/mS
= 80 mJ/mS

Table 2 shows comparison of power consumption resulting from the overhead due to intrusion detection algorithm for various number of nodes and cluster heads for the proposed system and normal sensor node based detection system

Table 2: Comparison of Power Consumption due to intruder overhead

No. of Nodes in the network	No. of Cluster heads in each network	Proposed Base Station based detection System (mJ/mS)	Normal Sensor Node based detection System (mJ/mS)
50	5	4	40
100	10	8	80
150	15	12	120
200	20	16	160
250	25	20	200
300	30	24	240
350	35	28	280
400	40	32	320
450	45	36	360
500	50	40	400

As shown in Figure 17, proposed system consumes negligible additional power for implementing intrusion detection based security solution. Also, it is very energy-efficient as compared to conventional sensor node based system.

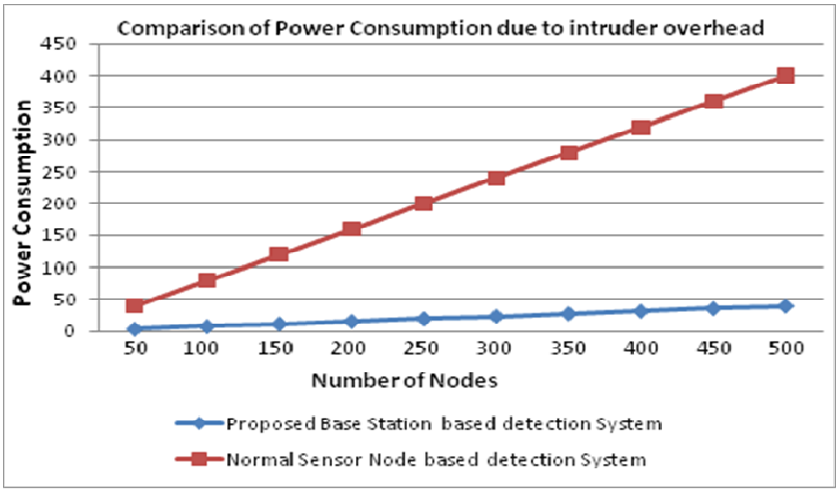


Fig : 17 - Comparison of Power Consumption due to intruder overhead

6. Conclusion

In this paper we have illustrated MAC address based intruder tracking system for cluster-based wireless sensor networks. This proposed system implements base station based detection and thus is very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by efficient security system can prevent many problems like slowing down of the network, sending of fake data, etc. By designing a security system in which the Base Station (BS) keeps track of the security

of the Wireless network, high security can be ensured without any significant energy overheads on individual nodes and cluster heads.

References

[1.] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.
[2.] R. Bace, "Intrusion Detection", MacMillan Technical Publishing, 2000.
[3.] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" *Journal of Theoretical and Applied Information Technology*, 2010, pp. 14-27.
[4.] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", *International Journal of Advanced Networking and Application (IJANA)*, Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.
[5.] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", *International Journal of Wireless & Mobile Networks (IJWMN)*, Aug. 2010, vol. 2, no. 3, pp. 49-61.
[6.] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks" *International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*, November 2010, vol. 1, issue no. 2, pp. 85-95.
[7.] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Routing Protocols in Wireless Sensor Networks – A Survey" *International Journal of Computer Science and Engineering Survey (IJCSES)*, November 2011, Vol. 1, issue no. 2, pp. 63-83.
[8.] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energy-efficient Routing Protocols for Wireless Sensor Network", *Global Journal of Computer Application and Technology (GJCAT),* Jan. 2011, vol. 1, no. 1, pp. 57-65.
[9.] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy Efficient Transmission Error Recovery for Wireless Sensor Network", *International Journal of Grid and Distributed Computing (IJGDC),* December 2010, vol. 3, no. 4, pp. 89-104.
[10.] I. Khalil, S. Bagchi, and C. Nita-Rotaru, "DICAS: Detection, diagnosis, and isolation of control attacks in sensor networks", in *Proceedings of the 1st IEEE International Conference on security and Privacy for Emerging A*reas in Communications Networks (SecureComm'05)*, Athens, Greece, Sept. 2005, pp. 89-100.*
[11.] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04)*, Washington, DC, Oct. 2004, pp. 66-77.
[12.] C.C. Su, K.M. Chang, Y.H. Kue, and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in *Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05)*, vol. 4, New Orleans, L.A., Mar. 2005, pp. 1927-1932.
[13.] Rodrigo Roman, Jianying Zhou, and Javier Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks"
[14.] Ruchi Bhatnagar, Dr. A.K. Srivastava, and Anupriya Sharma, "An Implementation Approach for Intrusion Detection System in Wireless Sensor Network", *International Journal on Computer Science and Engineering (IJCSE)*, 2010, vol. 02, no. 07, pp. 2453-2456.

Authors

Shio Kumar Singh is Head of Maintenance Engineering Department (Electrical) at Tata Steel Limited, Jamshedpur, India. He received degrees in both Electrical and Electronics engineering, as well as M.Sc.(Engg.) in Power Electronics from Regional Institute of Technology, Jamshedpur, India. He also obtained "Executive Post Graduate Diploma in International Business" from Indian Institute of Foreign Trade (IIFT), New Delhi, India. He is an accomplished academician with rich industrial experience in design, development, implementation and marketing & sales of IT, Automation, and Telecommunication solutions, Electrical & Electronics maintenance, process improvement initiatives (Six-sigma, TPM, TOC), and Training & Development in a distinguished

career spanning over 30 years. He has published more than 15 papers in both national and international journals and has presented these in various seminars and symposiums.

He is author of several engineering books such as Database Management System, Industrial Instrumentation and Control, and Process Control Systems published by Pearson Education, McGraw-Hill, and Prentice-Hall of India. He is widely traveled and has visited various industries in Europe and South Asian countries for study and marketing of process automation systems. He has been conferred the Eminent Engineer and Distinguished Engineer Awards by The Institution of Engineers (India) for his contributions to the field of computer science and engineering. He is a Chartered Engineers and also a Fellow Member (FIE) of The Institution of Engineers (India).

Dr. M. P. Singh is an Assistant Professor in the Department of Computer Science and Engineering at National Institute of Technology Patna, Bihar, India. He has experience of five years. He has authored number of papers which have been published in both national and international journals. His research interest is in the area of Wireless Sensor Network, Mobile Computing

Dr. Dharmendra K Singh is presently working as Head, Department of Electronics and Communication & Information Technology, BIT Sindri, Dhanbad. He has more than 20 years of teaching experience. He is heading the department of Electronics and Communication & Information technology since 2002. He is instrumental in starting the curriculum on information technology. He has published more than 50 papers in journals and conferences. He has already supervised 01 thesis in computer Science & Engg and 05 research scholars are presently enrolled for their doctoral degree. The area of research he works are Coding theory, cryptography, optical Amplifiers, Photonic Crystal Fibers, e-Governance and Educational Planning. He is member and conveners of various computerization programs of BIT Sindri, Vinoba Bhave University, Ranchi University. He is also a Fellow Member (FIE) of The Institution of Engineers (India).