IMPROVEMENT OF QUALITY OF SERVICE PARAMETERS USING REINVENTED FSMAC PROTOCOL FOR WIRELESS SENSOR NETWORKS

S. S. Agrawal[1], K. D. Kulat[2], M. B. Daigavane[3]

[1]*Assiatant Professor, Electronics and Telecommunication, SKNCOE, Pune, Maharashtra, India,*
[2]*Professor, Electronics and computer science, VNIT, Nagpur, Maharashtra, India*
[3]*Professor, Electronics and power Electronics, SD College of Engg., Wardha*
sujata.agrawal@rediffmail.com, kdkulat@ece.vnit.ac.in, mdai@rediffmail.com

Abstract

Now-a-days Wireless Sensor Networks (WSNs) have been used in a various applications including military and security monitoring, industrial control, health monitoring, home automation, intelligent agriculture and environmental sensing. The shared and easy to access medium is undoubtedly the biggest advantage of wireless networks. The shared nature of the medium in wireless Sensor Networks makes it easy for an attacker to launch a Denial of Service (DoS) attack. These attacks are happening to stop the legitimate node from accessing resources. There are many occasions where the attack can be much easier for an attacker. For example, in carrier sensing based networks (a) the transmissions at the sender are deferred because the medium is sensed to be busy, and/or (b) the reception at the receiver is interfered with due to the jamming signals. Both these effects degrade the wireless network performance significantly. As a result causes degradation in Quality-of-Service (QoS) of a sensor network. In proposed paper, Fuzzy Logic Secure Media Access Control (FSMAC) Protocol is reinvented using new intrusion detection parameter. These two parameters are Number of time channel sensed free and variation in Channel sensed period. Performance characteristics are measured in terms of successful data transmission rate and throughput of the network.

Keywords: *Wireless Sensor Networks, Denial-of-Service Attack, Quality of Service, Reinvented FSMAC Protocol.*

----------***----------

1. INTRODUCTION

Wireless Sensor Networks (WSN) are gaining lot of attention Because of its over increasing usage. WSNs are large network of Small, Battery-operated sensor nodes which are situated randomly in a vast geo-graphical area[1]. Denial-of –Service (DoS) Attack destroys the network resources so that sensor nodes behave unpredictably. These attacks are becoming very sensitive issue in WSNs. DoS Attack disturbs the balance between efficiency and fairness of common channel access [2]. The adoption of wireless sensor networks by applications that require complex operations, ranging from health care to industrial monitoring, has brought forward a new challenge of fulfilling the quality of service (QoS) requirements of these applications. QoS support is a challenging issue because of highly resource constrained nature of sensor nodes, unreliable wireless links and harsh operation environments. In this paper, we focus on the QoS enhancement at the MAC layer against DoS Attack. While the early research on WSNs has mainly focused on monitoring applications, such as agriculture and environmental monitoring, based on low-rate data collection, current WSN applications can support more complex operations ranging from health care to industrial monitoring and automation. This emerging application domain is that performance and quality of service (QoS) assurances are becoming crucial as opposed to the best-effort performance in traditional monitoring applications.

International Telecommunication Union (ITU) Recommendation E.800 (09/08) has defined QoS as: ‘‘Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service’’.

QoS brings the ability of giving different priorities to various users, applications, and data flows, frames or packets based on their requirements by controlling the resource sharing. Hence higher level of performance over others can be provided through a set of measurable service parameters such as delay, jitter, available bandwidth, and packet loss. Collisions and consequently retransmissions due to Dos Attack have direct impact the overall networking metrics such as throughput, delay and energy efficiency. Since the MAC layer coordinates the sharing of the wireless medium, it is responsible for minimizing the number of collisions.

Fuzzy Logic Secure Media Access Control (FSMAC) Protocol [3] gives good solution against DoS Attacks. It reduces the rate of false detection as well as increases the successful packet transmission rate.

In proposed paper, FSMAC protocol is re-established using new intrusion detecting parameters. These parameters are number of time node sensed free channel and Variation in channel sense period. FSMAC protocol first finds out the intrusion using pre-defined intrusion detector indicators. Fuzzy Logic (FL) is used innovatively for decision making. Appropriate countermeasures are taken to reduce the destruction of attacks basing on intrusion detection results. Simulations are carried in Matlab with 20 nodes to verify the effect.

The rest of the paper is arranged as following:
A survey of the research in security issues in sensor networks and overview on DoS Attack are presented in section 2. The Computational intelligence and Fuzzy Logic Theory is outlined in section 3. The structure of proposed FSMAC algorithm with new parameters is explained in section 4. The network scenario implemented in order to validate the secure MAC and results obtained are discussed in section 5. Finally the concluding remarks are made.

2. PRELIMINARIES

In this section, present security issues in wireless sensor network are discussed as well as DoS Attack is explained in brief.

2.1. Current Security Issues

Wireless links are very sensitive to passive eavesdropping, message replaying and message distortion. Weakly protected nodes that move into hostile environments can be easily compromised. Due to dynamic topology, authorization of administration becomes difficult. The scale of deployment of a WSN requires conscious decision about trade-offs among various security measures. These issues are discussed and mechanisms to achieve secure communication in WSNs are presented in [6]. Various security challenges in wireless sensor networks are analyzed and important issues that need to be addressed for ensuring adequate security are summarized in [7].

Secure routing is a major research area. Types of routing attacks and their countermeasures are presented in [8]. Researchers have proposed several methods of securing the MAC layer against the attacks by adversaries. DoS attacks and their countermeasures at the CSMA/CA MAC layer are discussed in [18] and [19].

2.2 Overview of DoS Attack

DoS attacks are classified into three groups: collision, unfairness and exhaustion attacks based on their mechanism.
In a collision attack, the attacker sends data packets regardless of the status of the broadcast medium. Such packets collide with the data or control packets from the legitimate sensor nodes. Using this mechanism, the collision only happens in the exchanging period of RTS and CTS packets, which means the data packet sending process is a non-collision process.

In an unfairness attack, for most RTS/CTS-based MAC protocols, each node has the same priority to get the common channel. The first tried node governs the channel. Besides, all other nodes have to wait for a random length time before trying to transmit packets. This rule could ensure that every node accesses common channel fairly. Adversaries could utilize these characteristics to attack the network. They send out packets just waiting for a very short time or without waiting. This causes the common channel used more by adversaries than by normal nodes. This is what we called unfairness attack. the adversary transmits an unusually large number of packets when the medium is free. This prevents the legitimate sensors from transmitting their packets.

In an exhaustion attack, the adversary transmits an abnormally large number of RTS packets to the normal sensor nodes, which exhausts them prematurely.

3. BACKGROUND TECHNIQUES

Under this Heading, techniques used against DoS Attack are discussed.

3.1 Computational Intelligence

Computational Intelligence (CI) is proper tool used to solve security problems of DOS Attack in wireless sensor networks. CI parameters are encouraged by nature. [2][3]. Different parameters of CI have been successfully used in past few years to address various challenges. CI provides adaptive mechanisms that exhibit intelligent behavior in complex and dynamic environments like WSNs.

CI works very flexibly, autonomously and robustly against dynamic topology changes, transmission failures and attacked scenario. CI fuses elements of learning, adaptation, evolution and fuzzy logic to create intelligent machines. In addition to paradigms like neural networking, reinforcement learning, evolutionary computing and fuzzy computing, swarm intelligence, artificial immune systems. Parameters of CI have found practical applications in areas such as product design, robotics, intelligent control, and biometrics and sensor networks. Researchers have successfully used CI techniques to address many challenges in WSNs [2] [10].

The literature has a few articles that use CI approaches for WSN security. The applications available in the literature have handled the issue of Denial-of-Service (DoS) attacks at the node level. Individual sensor node is resources- energy, bandwidth, computation, memory constrained device. Therefore, algorithms that involve high computational and storage burdens are not attractive. So Fuzzy logic and compact NNs are among solutions discussed.

3.2. Fuzzy Logic

Human reasoning includes measure of imprecision and uncertainty where as Set theory allows elements to be either included in a set or not. Human reasoning is marked by the use of linguistic variables like most, many, frequently, seldom etc. This approximate reasoning is modeled by fuzzy logic. Fuzzy logic is a multivalued logic that allows intermediate values to be defined between conventional threshold values [15].

Fuzzy systems allow the use of fuzzy sets to draw conclusions and to make decisions. Fuzzy sets differ from classical sets in that they allow an object to be a partial member of a set. In fuzzy systems, the dynamic behavior of a system is characterized by a set of linguistic fuzzy rules based on the knowledge of a human expert. Fuzzy rules are of the general form:

IF antecedent(s) THEN consequent(s)

Where antecedents and consequents are propositions containing linguistic variables. Antecedents of a fuzzy rule form a combination of fuzzy sets through the use of logic operations [3]. Thus, fuzzy sets and fuzzy rules together form the knowledge base of a rule-based inference system as shown in Fig 1 [3].

Fig. 1 shows the structure of a fuzzy logic system (FLS) [15]. When an input is applied to a FLS then the inference engine computes the output set corresponding to each rule. The defuzzifier then computes a crisp output from these rule output sets [3] [11].

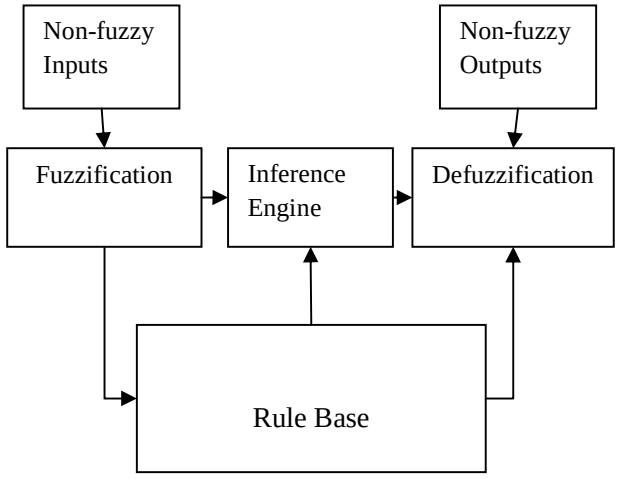

Fig-1: Fuzzy Inference Engine

4. PROPOSED FSMAC ALGORITHM

This section discusses design of FSMAC protocol algorithm with new parameters.

4.1 Selection of Intrusion Detector

When collision attack intrudes the network, attackers send massive packets into the common channel when detecting this channel is busy. As a result, more RTS, CTS, ACK and even data packets may be destroyed. Due to the collisions caused by attackers. See Fig. 2. Moreover, the average latency of data packet is prolonged because of more retransmitting control packets and data packets [4] [9].

Under normal condition, without any attacks, it is fair for each node to transmit data over the common channel from long-term statistic view. Since nodes have to wait for a random time before sending RTS to try to hold the common channel. Only the first successful one can be allowed to transmit data over the common channel. Data packets of normal sensor nodes are supposed to wait longer time at MAC layer, when unfairness attackers prevent other normal sensor nodes from transmitting. This is done by holding the channel ahead of time [3][8].

Differing from collision attack and unfairness attack, exhaustion attackers work almost same as other normal sensor nodes, except for sending RTS repeatedly to some normal sensor nodes. As a result, the arrival rate of RTS at victim nodes will increase dramatically. Besides this, data packets should wait longer time, since the common channel is more utilized for transmitting RTS by attackers [4].

As well as for unfairness attack as the channel is free, attacker is ready to attack which causes an attack. There is specific

time for transmitting RTS to the receiver, but at the time of exhaustion attack, because of large number of RTS are sent over receiver, length of that period gets minimized.

From above analysis, it shows that the intrusions may be detected by monitoring abnormal alterations of some sensitive network parameters. They are:

- A great number of RTS packets are received by victim nodes for exhaustion attacks.
- Average waiting time becomes very long for both unfairness attacks and collision attacks.
- Collision takes place considerably often in collision attacks.
- When more the times channel is sensed free by a certain node, possibility of intruded DOS Attack is high and vice-versa.
- If channel sense period is more possibility of attack will be less.

By observing abnormal changes in No. of times node sensed free channel and Variation in channel sense period.
In this paper, chosen parameters are as follows:

- Number of times node sensed free channel.
- Variation in channel sense period.

4.2 FSMAC Algorithm Description

Fig. 2 shows the mechanism of the proposed secure MAC algorithm. There are addition of two modules-intrusion and defense module into original CSMA/CA protocol.

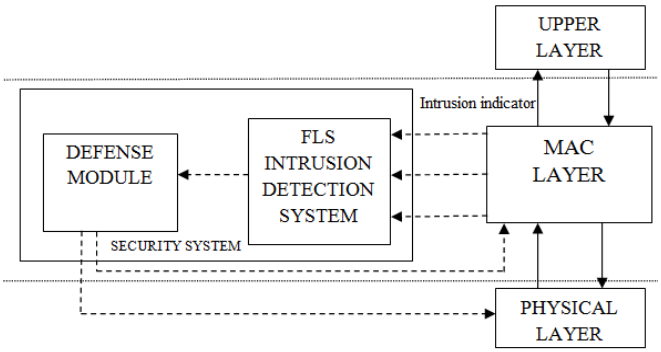

Fig-2: Intrusion Detection System

Each sensor node is provided with it's own security system.In FSMAC, intrusion module of each sensor node monitors the intrusion detection parameters and periodically checks whether intrusion happens or not. If intrusion is happened then the defense module of the sensor node will be triggered by Fuzzy Logic System (FLS) intrusion detection module. Defense module will inform physical layer and Mac layer to switch to different Radio Frequency (RF) band to start or stop the transmission. This sensor node will get back to the original RF band or restarts information exchanging over network after this period, as well as intrusion detection will be resumed.

Each sensor node monitors, Free sensed channel and Channel sense period, which are the inputs or antecedents of FLS intrusion module. Then according to the output or consequent possibility of intrusion found of FLS intrusion detection module, security systems make a decision whether the intrusion exists or not.

For proposed FLS, linguistic variables or antecedents are used to represent, Number of times Channel sensed free and variation in Channel sense period. These antecedents are divided into three levels i.e. Low, Moderate, High. The output i.e. Possibility of intrusion detection is divided into five i.e. Very Low, Low, Moderate, High, Very High. As every antecedent has three fuzzy subsets and there are two antecedent, 6 possibilities of consequents.

From behavior of these inputs the paper may discuss the behavior of consequents i.e. possibility of intrusion applying Fuzzy Logic as follows:
Antecedent 1: Number of times Chanel is sensed free.
Antecedent 2: Variation in Channel Sense period.
Consequent: possibility of intrusion Detection.

Table-1: The rule base for intrusion detection.

Antecedent 1	Antecedent 2	Consequents
Low	Low	Very High
Low	Moderate	High
Moderate	High	Moderate
Moderate	Low	Moderate
High	Moderate	High
High	High	Very Low

A defense module is trigged, when intrusion is found. Defense module takes countermeasures to reduce the effects of attackers on the network.

During the intrusion period, it is an energy waste or unsafe action for normal sensor nodes to transmit or receive. Because the transmitting or receiving is almost unsuccessful or spied by attackers when enemies attack the network Thus it is an appropriate and effective choice for the normal nodes to switch to a different RF band to make transmission or to stop transmitting and receiving.

The paper focuses on intrusion detection and increasing the lifespan of protocol. For example, if it choose stopping transmitting and receiving mechanism to implement defense function There is no information on attacks duration, it can't make the node sleep until attacks stop. So, after a period of sleep, this node should wake up to make data transmission and detect the intrusion again. This node will stay at this state until

intrusion is found again. At sleep mode, there is no transmitting and receiving, bModrut sensing still continues.

In order to make new secure algorithm, this has no centre control available for general WSNs. This defense scheme, like intrusion detection scheme, is also distributive i.e. each sensor node's defense schedule has no any relationship with other sensor node's [3]

5. RESULTS AND DISCUSSION

5.1. Simulation Setup

The paper runs simulations using MATLAB simulator. Thirty sensor nodes are deployed randomly in an area of l km X l km, and communication range (radius) is 500m. Nodes are set to be initially with energy of 2 J. The destination for each sensor node will be randomly chosen.

First it checks the behavior of CSMA/CA protocol and then it separately tests the influences of each DoS attack i.e. collision attack, Unfairness attack and Exhaustion attack on CSMA/CA protocol. In each experiment, there is only one type of attack introduced. The attacker is an abnormal sensor node, which has been captured and reprogrammed by enemies successfully before the system starts to work.

5.2 Simulation Results

Parameter metrics are defined to testify the effects of our algorithm. It is,

- Possibility of successful detection (P_d): P_d is the possibility of nodes making correct detection.
- Possibility of false detection (P_{fd}): P_{fd} is the possibility of nodes making false detection.
- Data packet successful transmission rate (R_{st}): R_{st} is the rate of successfully transmitted data packets to all data packets transmitted.
- Throughput: It represents the total number of packets received successfully by a receiver per second. It can also be defined as the total amount of data a receiver actually receives from sender divided by the time taken by the receiver to obtain the last packet. It also represents the packet overhead within the route.
- Graph of Successful packet transmission are shown below:

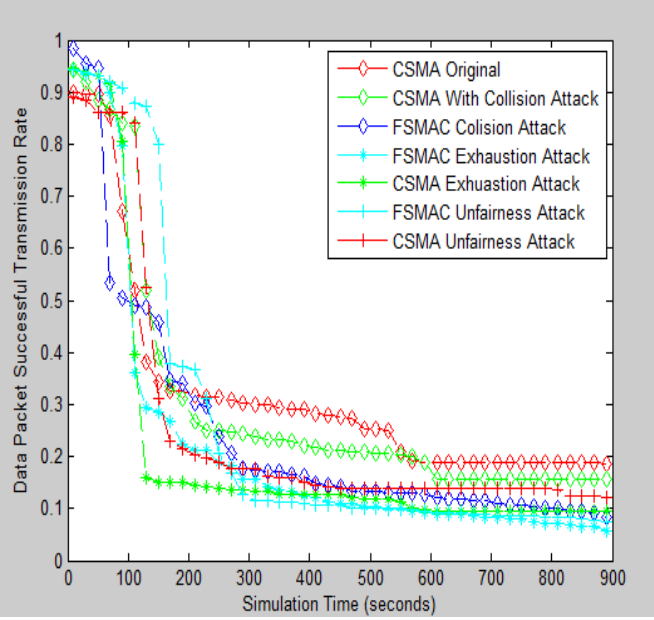

Fig-3: Graph of successful data transmission with FSMAC protocol having 3 intrusion detection parameters.

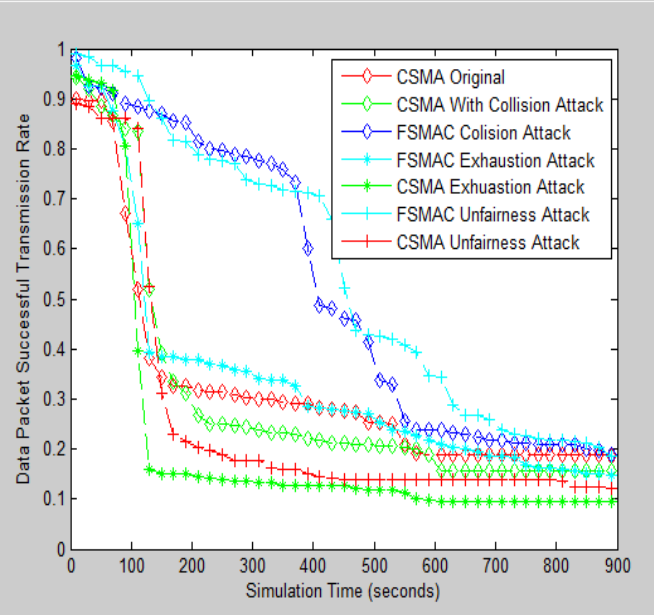

Fig-4: Graph of successful data transmission for reinvented FSMAC protocol having 2 intrusion detection parameters.

From above graph, it is observed that rate of successful data transmission is more for reinvented FSMAC protocol and combined protocol than Attacked CSMA/CA protocol and existing FSMAC protocol.

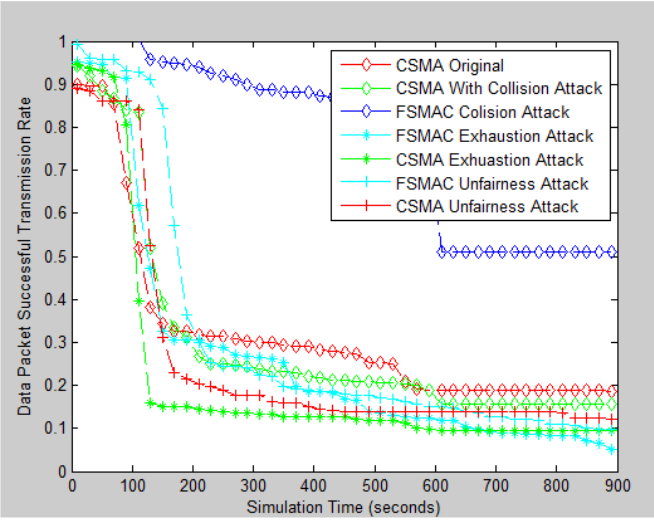

Fig-5: Graph of successful data transmission for FSMAC protocol having 5 intrusion detection parameters.

Throughput for CSMA/CA without any Attack is 92.80% Throughput for different DoS Attacks are calculated as follows:

Table-2: Throughput for Collision Attack

CSMA/CA	FSMAC (Existing)	FSMAC (Reinvented)	FSMAC (Combined)
68.41%	81.68%	92.33%	90.29%

Table-3: Throughput for Exhaustion Attack

CSMA/CA	FSMAC (Existing)	FSMAC (Reinvented)	FSMAC (Combined)
76.64%	89.73%	88.90%	90.30%

Table-4: Throughput for Unfairness Attack

CSMA/CA	FSMAC (Existing)	FSMAC (Reinvented)	FSMAC (Combined)
75.61%	86.61%	94.86%	88.98%

CONCLUSIONS

From above study, it shows that, reinvented FSMAC protocol gives good performance against Dos Attack and following Conclusions are made:

1. FSMAC protocol with pre-defined new parameters gives better detection than existing FSMAC protocol.
2. Rate of Successful data transmission is increased for reinvented as well as for combined FSMAC protocol.
3. Throughput is remarkably increased for reinvented FSMAC protocol in case of Collision and Unfairness Attack.

ACKNOWLEDGEMENTS

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1]. Xiuli Ren and Haibin Yu, "Security Mechanisms for Wireless Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.3, March 2006.

[2]. Raghavendra V. Kulkarni, Anna Förster, and Ganesh Kumar Venayagamoorthy "Computational Intelligence in Wireless Sensor Networks: A Survey" IEEE Communication Surveys & Tutorials, VOL. 13, NO. 1, First Quarter 2011.

[3]. Qingechun Ren and Qilian Liang ,"Fuzzy Logic-optimized Secure Media Access Control (FSMAC) Protocol for Wireless sensor Networks" CIHSPS-2005 IEEE International Conference on Computational intelligence for Home and Security and Personal Safety 2005.

[4]. Alberto Lopez Toledo and Xiaodong Wang, "Robust Detection of MAC layer Denial-of-service attacks in CSMA/CA Wireless Networks", IEEE Transactions on Information Forensics and Security,Vol.3 No.3 September 2008 .

[5]. Taimur Farooq,David lewellyn-Jones Madjid Merabti,"MAC layer DOS Attack in IEEE802.11 Networks",location:Liverpool Jon Moores University K.ISBN:978-1-902560-24-3, April 2010.

[6]. E. Shi and A. Perrig, "Designing secure sensor networks," IEEE Wireless Commun. Mag., vol. 11, no. 6, pp. 38-43,2004.

[7]. F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," Ad Hoc Networks, vol. 3, no. 1, pp. 69-89, 2005.

[8]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's AdHoc Networks Journal,Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2-3, pp. 293-315, September 2003.

[9]. A. R. M. Kamal, "Adaptive secure routing in ad hoc mobile network," Master's thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, Nov 2004.

[10]. Jethro Shell, Simon Coupland, Eric Goodyer "Fuzzy Data Fusion for Fault Detection in Wireless Sensor Networks" ISBN 2010.

[11]. Vikram Gupta, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks", Proceedings of MILCOM 2002, vol. 2, 7-10 Oct.2002.

[12]. Yihong Zhou, Dapeng Wu ,Scott M. Nettles, "Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems" ISBN 2004.

[13]. Hongfa Wang , "A Robust Mechanism for Wireless Sensor Network Security" IEEE Conference on wireless communication 2010.

[14]. John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson "Fuzzy Intrusion Detection" Joint 9th IFSA

world congress and 20th NAFIPS International conference VO.4 2001, PP 2165-2170.
[15]. H. Chan, A. Perrig, “Security and Privacy in Sensor Networks ," Oct. 2003, pp. l 03 - IOS.
[16]. O. Kacllirski, R. Gulla, " Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks ," SFGCOMM '03, Aug. 2003.
[17]. Anthony D.Wood and Jon A. Stankovic,“Denial-of Service attacks in sensor network”.
[18]. Adam Stubblefield. John Ioannidis, Aviel D. Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”.
[19]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”.

BIOGRAPHIES

Sujata S Agrawal completed her B.E(E&T.C) Degreefrom Nagpur University in 1992 and ME degree in 2005from Government college of engineering, Aurangabad.She is persuing her Ph.D. degree in Electronics Engineering from RSTMNagpur University, India.Having a total experience of 14 years, she is currently associated with Smt.Kashibai Navale college of engineering, Pune as Assistant Professor in the Electronics & telecommunication Department. She is the Life Member of the Indian Society for technical Education.

Kishore D. Kulat completed his degrees in Electrical Engineering, BE in 1980, from VRCE (at present VNIT) Nagpur and ME degree in 1984 from VJTI, Mumbai, India. He completed his Ph.D. degree in Electronics Engineering, in the year 2003 from VNIT, Nagpur. Having a total experience of more than 25 years, he is currently associated with VNIT, as Professor in the Electronics & Computer Science Department. With his profound knowledge & experience in his field he is guiding around 15 research scholars for their doctoral degree. Two have been awarded the Ph. D. degree. He has published around 15 Journal Papers, more than 25 papers in International Conferences & more than 40 have been published in National Conferences. Has worked as Reviewer for many National & International conferences.He is a member of Board of Studies for Electronics Engineering, Nagpur University for last 10years. He is member of Professional societies like IETE, IEI and ISTE. With all his faith in God, Dr. K. D. Kulat believes in achieving excellence through the process of continuous upgradation.

Manoj B. Daigavane obtained the B.E. Degree in Power Electronics Engineering from Nagpur University, India in 1988.He received the M.S. Degree in Electronics and Control Engineering from Birla Institute of Technology and Science, Pilani (Raj) India in 1994. He also obtained the M.E. Degree in Power Electronics Engineering from Rajeev Gandhi University of Technology, Bhopal (M.P), India in 2001. He received Ph D Degree in Electrical Engineering from RSTM Nagpur University, India in 2009. Since Sept.1988- June 2007, he had been with the Department of Electronics and Power Electronics Engineering, B.D.College of Engineering, Sewagram (Wardha), affiliated to the Nagpur University, India. Since July 1, 2007 toApr 30, 2009, he was Professor & Head of Electrical and Electronics Engineering, Disha Institute of Mgmt. andTech., Raipur (C.G.) where he is engaged in teaching & research. Presently, he is Principal of S. D. College of Engineering, Wardha – Maharashtra (India), since May 01, 2009. His main areas of interest are Design of electronic circuit, resonant converters, Power quality issues, DSP applications and Power electronics for motor drives. He has been responsible for the development of Electrical Machines and Power Electronics Laboratories He is a Member of the Institution of Engineers (India) and a Life Member of the Indian Society for technical education.