DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5553

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A FRAMEWORK FOR COMPARATIVE ANALYSIS OF WSN ATTACKS AND COUNTER MEASURES RECOMMENDATIONS

Mohammed Abdul Azeem
Research Scholar, CSEDJNTU,
Hyderabad, India

Dr. Khaleel-ur-Rahman khan
Professor, CSED ACE Engg College,
Hyderabad, India

Abstract: The growth in the need for customized services in hand held devices and sensor based applications are continuously motivating the wireless networks, wireless communications and wireless infrastructures. In the last decade the wireless communication has evolved around the MANETs and IoT devices. Nevertheless, the demands for wireless sensors have not decreased due to less costly and simple deployments measures. The wireless networks especially running on the tiny operating systems are designed and programmed to perform very specific tasks. Also, the processing capabilities of these devices are limited. Henceforth, it is difficult to incorporate additional services into the devices such as routing management, data processing or security. The routing management protocols or the data processing frameworks are often the essential part of the framework. Nevertheless, due to the bottleneck between performance and service availability, the service providers ignore the security issues. Considering the wide use of the wireless sensors ranging from healthcare to tactical usage, it is the demand of the modern research to re-address the security measures of the wireless sensor network. In the recent past, the researchers and practitioners have witnessed a number of attacks on WSN infrastructures and policies. The attacks were diversified in terms of distortions of the information, damage to the network or sometimes vulnerability to the user identifications. Hence, none of the single frameworks are capable of detect all types of attacks on WSN. It is been observed that during any attacks on the WSN, the parametric values related to power, energy and response time changes drastically. Henceforth, any measure of the changes and continuous monitoring may lead to finding a pattern in the data tenting to standard formulations. Thus this work proposes a novel framework to detect the behavioural malfunction of the wireless sensor networks based on the energy, power consumption and response time of the nodes. This is proposed to be the major outcome of this work. Yet another novel outcome of this work is to associate the detection model with the attack response knowledge base in order to generate timely recommendations to avoid the damages. The objective of this work is to create a responsive system for controlling the damages caused by any attack on wireless sensor network for making the world of wireless communication more trustable.

Keywords: WSN, Interrogation, Energy Drain, Hello Flood, Misdirection, Flooding, Jamming, Collision, Black Hole, Denial of Service, Selective Forwarding, Attack Simulation, Network Parameters, Attack Detection, Counter Measures

I. INTRODUCTION

The demand for the smart infrastructure is continuously growing in healthcare, buildings, agriculture, and industrial automation and in all other verticals.Henceforth, the research in wireless smart sensing technology is witnessing a massive deployment of the sensors in all these areas. The demand is not only for the data accumulation, rather processing the information and using the results for different decisive factors as well. The data accumulation is majorly dependent on the wireless sensors along with communicating the data to the central processing locations. The uses of wireless sensors are wide due to its capability of low cost, high energy consumption and the capacities of moderately wide seamless deploy ability. Nevertheless, the wide deployment of the wireless sensors, away from visible monitoring range makes the network vulnerable to the security threats. The work by Kavitha et al. [1] has demonstrated the possibilities of attacks on any wireless sensor network due to the fragile security protocols. Thus it is the responsibility of the wireless network service provided to deploy security measures on the central processing locations in order to reduce the damages caused by the attacks.

The architectures for the WSNs are standard and have specific standardization for the sensor node, network protocols and the data processing system. The specifications for these factors are decided by the demand of the purpose, the network is deployed for. Nonetheless, the demand for the security measures cannot be pre-determined as the attacks do not rely on network type or sensor type or the type of the data. The wireless sensor network devices after deployed might be kept unattended and thus the demand for the security is a primary concern. The other types of computing networks are also vulnerable to attacks. But due to the shared, unprotected communication channels, limited computing capabilities, low power leverage and low system complexity, the wireless sensor networks attract more security threats than the usual networks.

The demand for the security measures can be claimed by the customers or the beneficiaries based on the type of application are deployed using the network. Also various types of attack leave different footprints on the system and make significant damage to the network [Fig.1].

Thus it is important to realize the effects of the attacks on the sensor networks.

While designing the security measures for any sensor networks, the memory limitations, computational capabilities, power consumption, distribution factors and the communication or routing algorithms must be taken under consideration. It is natural to realise that there is no single solution to all types of attacks; rather the detection mechanism can be designed in order to detect the presence of the attack on the system.

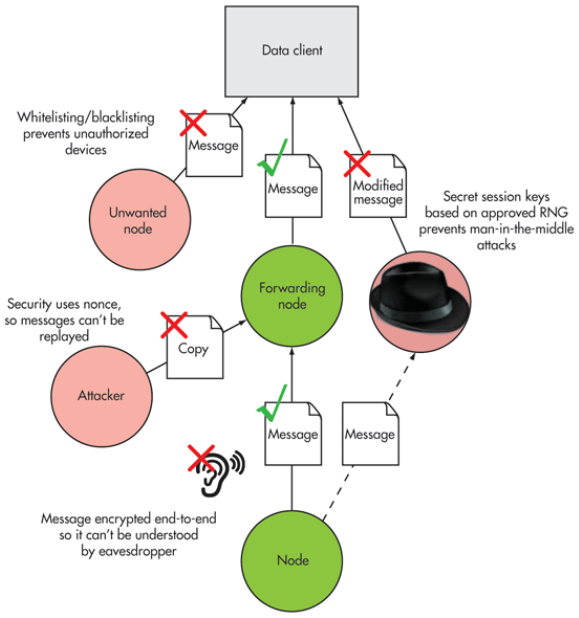

Fig.1 Example of any attack on Wireless sensor Network

Thus this work proposes a framework for determining conditions of various parameters during the major types of attacks. A number of parallel researches have attempted to standardise the nature of the attacks and classified in various groups. The work by Padmavathi et al. [2] has demonstrated the security measures and challenges to be addressed on wireless sensor network. Recommending the counter measures are also a popular trend in the research directions as attempted by Malik et al. [3]. Few of the parallel researches have demonstrated a different approach towards preventing the attacks, rather than detecting the attack. The notable work by Shukla et al. [4] elaborated the defence mechanisms possible on WSN. The type of attacks on WSN and MANET are not very different in nature. The work by Nguyen et al. [5] has demonstrated the similarities of WSN and MANET attack classifications and similarities. Data accumulation is the major task in any sensor network and there are some attacks which are intended to add noise to the data. The work by Mohanty et al. [6] has demonstrated some attack behaviours which causes noise to the data in the network. There are also some standard outcomes from the parallel researches and can be considered as literature on this work as the work by Han et al. [7] and Lupu et al. [8].

The major challenge of the research is to simulate majority of the attacks and understand the change in sensor network characteristics. Henceforth, this work proposes a framework to simulate few popular types of attacks and furnish the parametric change in the network.

The rest of the work is furnished such that in the Section – II the current understanding of the attacks and the simulation possibilities are considered, in the Section – III popular attacks and expected damages are considered, in the Section – IV the attack simulation and modelling methods are elaborated, in the Section – V the proposed framework for accumulating the effected parameters from the attack is elaborated, the driving algorithm for the proposed framework is furnished in the Section – VI, the results obtained from the framework with the counter measures are discussed in the Section – VII and the work presents the final conclusion of this work in the Section – VIII.

II. OUTCOME OF THE PARALLEL RESEARCH

The general nature of any attack is to gain unauthorized access to the resources like network services or the data or tamper the service confidentiality.The major types of attacks are described in the work by Mohammadi et al. [9].

The popular types of attacks as classified are Jamming Attacks, Interrogation Attacks, Hello Attack, Misdirection Attacks, Sybil Attack, Application Attack, Tampering Attack and Denial of Service Attack. Majority of the parallel researches have demonstrated either a single types of attack or simulation of a network scenario. The work by M. Mekni et al. [10] has significantly listed the network simulation tools with the reference to the works by Information Science Institute [11] and NESG [12]. Nonetheless, these simulators are not capable of simulating the attacks on the wireless networks. It is expected to model the attacks in these simulation tools to manipulate the network parameters. The expectations from the research are to have capabilities to accept the attack algorithms and understand the differences in the parametric values.

There are several simulators proposed by the parallel research attempts in the recent progress of the research. The works by Chhimwal et al. [13] on the features of the simulation tools, Pathan et al. [14] on technologies and methodologies of the simulation tools and Sarkar et al. [15] on the attack modelling techniques have given significant knowledge to the literature.

The widely accepted wireless sensor network simulation works are the network simulator or NS2 [16], NS3 [17], Cooja [18], Castalia [19], OMNET++ [20], GloMoSim [21], TOSSIM [22] and Avrora [23].

There are multiple other works which improved the usability and readability of these simulation strategies. The NS2 and NS3 based simulator by Petrioli et al. [24] called the SUNSET, the PARSEC by Bagrodia et al. [25], UML – RT based modelling oriented simulator by Peng et al. [26], discrete event simulation TinyOS [27], java based network simulator proposed by Sobeih et. al. called J-SIM [28], UWSim proposed by Dhurandher et al. [29], Prowler [30] and JProwler [31] proposed by Simon et al. are the significant once.

The functional capabilities of the popular and open source simulators are listed here [TABLE-I].

TABLE-IFUNCTIONAL CAPABILITIES OF POPULAR SIMULATORS

Simulator	Characteristics						
	Traffic Simulation	Application Simulation	H/W Simulation	OS Simulation	Power Measure	Security Recommendation	Availability
NS-2	Yes	No	No	No	Yes	No	Free Source
NS-3	Yes	No	No	No	Yes	No	Free Source
TOSSIM	Yes	No	No	Yes	No	No	Free Source
UWSIM	Yes	No	No	No	Yes	No	Free Source
AVRORA	Yes	No	No	No	Yes	No	Free Source
CASTALIA	Yes	No	No	No	Yes	No	Free Source
GLOMOSIM	No	No	No	No	No	No	Free Source
SHAWN	No	No	No	No	No	No	Free Source
J-SIM	No	No	No	No	Yes	No	Free Source
PROWLER / JPROWLER	Yes	No	No	Yes	No	No	Free Source
ATEMU	Yes	Yes	No	No	Yes	No	Free Source
OMNET++	Yes	Yes	Yes	No	Yes	No	Free Source
COOJA	Yes	No	Yes	Yes	Yes	No	Free Source

Henceforth, in the light of the knowledge on the popular simulation tools, it is natural to understand that the major demands to be addressed are:

- The demand for a single framework to simulate evaluate the attacks are to be proposed
- The change in the network parameters are to be identified during any specific or group of attacks
- The damage control security measures are to be proposed automatically based on the attack types

Furthermore, this requires the detailed analysis of the known attacks and possible changes in the network parameters. Thus the next section of this work elaborates the attack types.

III. POPULAR ATTACKS ON WSN

The attacks are classified based on the damages caused to the network infrastructures. In order to understand the implications for each network parameters, in this section or the work, the popular attacks are been studied and the influence on the network parameters are listed.

A. Interrogation Attack

This attack repeatedly sends RTS messages to any selective node in order to drain the resources and received the CTS responses.

B. Energy Drain Attack

This attack introduces high amount of network traffic in order to drain the energy of any network and as a result the number of dead nodes increases in the network. The types of drain attacks are surveyed by Dubey et al. [32] and presented in comparative framework.

C. Hello Flood Attack

This attack sends huge pile of “Hello” packets in the network by broadcasting and as a result the life time of the network reduces significantly. The types of flood attacks are surveyed by Singh et al. [33] and presented in comparative framework.

D. Misdirection Attack

The main objective of the intruder is to misdirect the incoming messages to increase the latency, which prevents a few packets from reaching the base station. It is been observed by the work of Abdullah et al. [34] that this attack can be identified by the nodes receiving data packets out of the regular pattern.

E. Flooding Attack

The main purpose of this attack is to deliberately communicate to a single node in order exhaust the resource limit or the connection limit. Yet another contribution by Dubey et al. [35] has demonstrated the classifications and implications.

F. Jamming Attack

This attacks cause denies of connection or access requests by the authorised clients of the network. The types of the jamming attacks are classified by Pelechrinis et al. [36] as an outcome of his popular survey.

G. Collision Attack

The collision attacks are introduced by sending a data packet with noises in order to disrupt the actual transmission. The collision attacks are extensively studied and presented by Reindl et al. [37].

H. Black Hole Attack

The black hole attacks cause a high packet loss in the network. This attack types alter the routing protocols in order to divert all packets to a specific node and then discard the packets. The black hole attacks are been deeply examined and presented by Ramaswamy et al. [38].

I. Denial of Service Attack

The widely encounter attacks are the DoS attacks and this attack type can damage any resource of the network. The varieties of this attack type were thoroughly studied and presented by J. Ding et al. [39].

J. Selective Forwarding Attack

The selective forwarding attack can often be confusing with the firewall protocols as certain nodes refuses to forward few packets in the network causing interruption in the service or the broadcasts. This phenomenon was elaborated by Y. Zhang et al. [40].

Henceforth, as outcome of the literature survey, this work presents the impact of each popular attack on the network parameters in order to build the proposed framework with the recommendation system [TABLE-II].

TABLE-II TYPES OF ATTACKS WITH INFLUENCE ON NETWORK PARAMETERS

Attack Type	Energy	Delay	Routing Pattern	High Traffic	Dead Node
Interrogation	Yes	No	No	Yes	No
Energy Drain	Yes	No	No	Yes	Yes
Hello Flood	Yes	No	No	No	Yes
Misdirection	No	No	Yes	Yes	No
Flooding	Yes	Yes	No	Yes	Yes
Jamming	No	No	Yes	No	No
Collision	No	Yes	No	No	No
Black Hole	No	No	Yes	No	No
Denial of Service	No	No	Yes	No	No
Selective Forwarding	No	No	Yes	No	No

Thus this measure will certainly help in order to model the attacks during simulation and build the proposed framework.

IV. ATTACKS MODELLING

For building the proposed framework, it is important to formulate the attack modelling metric. The proposed framework is intended to simulate the attacks and understand the implications on the network parameters [Table -2]. Thus this section of the work proposes the metric for attack modelling [TABLE-III].

TABLE-III ATTACK MODELLING METRIC

Attack Type	Modelling Strategy
Packet Inclusion Attacks	These types of attacks introduce large number of additional packets in the network. Thus during the modelling of the attacks it is proposed to include additional flooding sources in the network
Noise Inclusion Attacks	These types of attacks introduce noise in the captured data by the sensors. Thus during modelling these attacks it is intended to include pre-processing modules to add noise.
Firmware Attacks	These types of attacks are intended to manipulate the firmware services. Hence in order to simulate these attacks it is proposed to introduce denial of any resources in the network.

Thus, this proposed metric will help in simulating the attacks. Any possible combinations of these three strategies will help in simulating any types of attacks to the network.

V. PROPOSED FRAMEWORK

The proposed framework is motivated by the lack of sufficient researches in attack identifications and counter measures recommendations.This proposed framework is capable of simulating a majority of the popular researches and identifies the change in the network. The component based design of the framework makes it highly flexible for incorporating any new types of attacks or incorporating any new service types or any new network protocols [Fig.2].

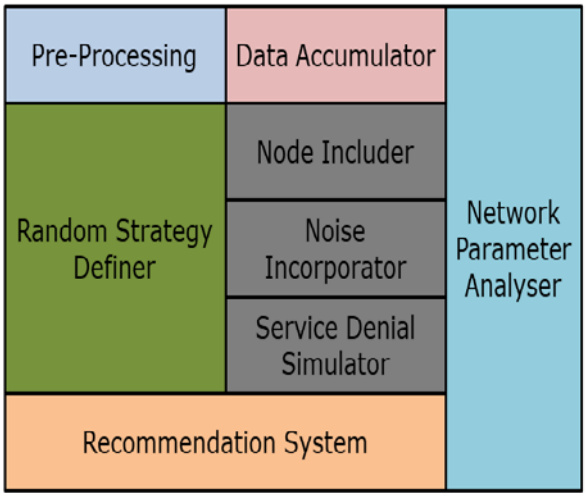

Fig.2 Proposed Framework for WSN Attack Simulation and Counter Measures

The components of the proposed framework are elaborated here:

A. Pro-Processing Component

The first component in the framework is the pre-processing component. This component generates data noises to be incorporated in the data collected from the sensor networks. The below furnished algorithm is used to incorporate the noise.

Algorithm 1: Noise Incorporation
Step -1. Accept the data signal
Step -2. If the signal is already noisy
Step -3. Then feed the data signal into the framework
Step -4. Else,
Step -5. Incorporate the noise signal as final_signal = input_signal XOR sin(input_signal)/mod(input_signal)
Step -6. Feed the data signal into the framework
Step -7. End

The algorithm is visualised here [Fig.3].

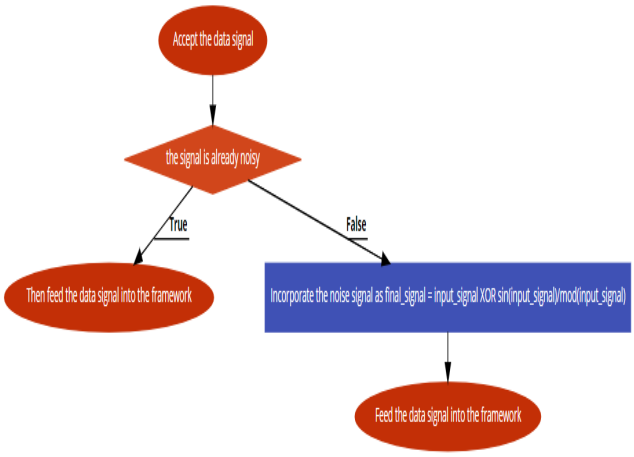

Fig.3 Proposed Noise Incorporation Algorithm

B. Data Accumulator Component

The second component is the data accumulator component. This component is not intended to collect data from the sensors, rather intended to collect simulation parameters from the sources, mostly test input files, for specified inputs. The detailed descriptions about the parameters are furnished here [TABLE-IV].

TABLE-IV SIMULATION & NETWORK PARAMETERS

Simulation Parameters	Parameter Description
DimentionX	The dimension of area for simulation in X axis
DimentionY	The dimension of area for simulation in Y axis
NumberOfNodes	Number of Nodes in the simulation
InitialEnergy	Initial energy for each node
NumberOfRounds	Number of simulation rounds
EnergyPerRound	Energy consumptions per round of simulation
Routing_Algorithm	The routing algorithm for the WSN during simulation
NumberOfDeadNodes	Number of Dead nodes per rounds
CommunicationTime	The simulation time per round

C. Random Strategy Definer Component

This component of framework defines combinations and the values for parameters. Based on the defined strategies, the attacks on the network will be simulated.

D. Node Includer, Noise Incorporator and Service Denial Component

Based on the feedback given by the strategy component these components will generate the nodes, noise and denial of services.

E. Network Parameter Analyser Component

The Network Performance Analyser Component continuously monitors the values of the simulation and network parameters. Based on the values, this component generates the possible attack type list. The algorithm deployed in this component of the framework is furnished and elaborated in the next section of this work.

F. RecommendationSystem

The final component of the framework is the recommendation system. This component will generate the countermeasures for the popular attacks automatically. In this part of the work, the countermeasures are listed [TABLE-V].

TABLE-V AUTOMATIC COUNTER MEASURES FOR THE ATTACKS

Attack Type	Recommended Counter Measures
Interrogation	• Disconnect the Node having highest traffic generated for a time slice
Energy Drain	• Check the traffic pattern for the selected node. • Analyse the routing table for exclusion of the dead node
Hello Flood	• Disconnect the Node having highest traffic generated for a time slice
Misdirection	• Check for the firewall policies • Check for the recent included new node policies
Flooding	• Disconnect the Node having highest traffic generated for a time slice
Jamming	• Check for the firewall policies • Check for the recent included new node policies
Collision	• Check for the recent included new node policies
Black Hole	• Check for the firewall policies
Denial of Service	• Check for the firewall policies • Check for the recent included new node policies
Selective Forwarding	• Check for the firewall policies • Check for the recent included new node policies

VI. ATTACK DETECTION ALGORITHM

In this section of the work, the algorithm for detecting the attack situations is furnished.

Algorithm 1: Attack Situation Detection
Read the initial network parameters Update the node list Replicate routing table Start the detection module Accumulate initial_energy Accumulate communication_time Accumulate number_of_deadnodes

Accumulate node_access_frequency
For Each round of communication
Detect the change in initial_energy
If change in initial_energy>energy_change_threshold
Notify the recommendation system as attack
Else,
Detect the change in communication_time
If change in communication_time>communication_time_change_threshold
Notify the recommendation system as attack
Else,
Detect the change in number_of_deadnodes
If change in number_of_deadnodes>number_of_deadnodes_change_threshold
Notify the recommendation system as attack
Else,
Detect the change in node_access_frequency
If change in node_access_frequency>node_access_frequency_change_threshold
Notify the recommendation system as attack
End
End

Based on the recommendation generated from this algorithm, the recommendation system will suggest the counter measures for the attacks.

The algorithm is visually analysed here [Fig.4].

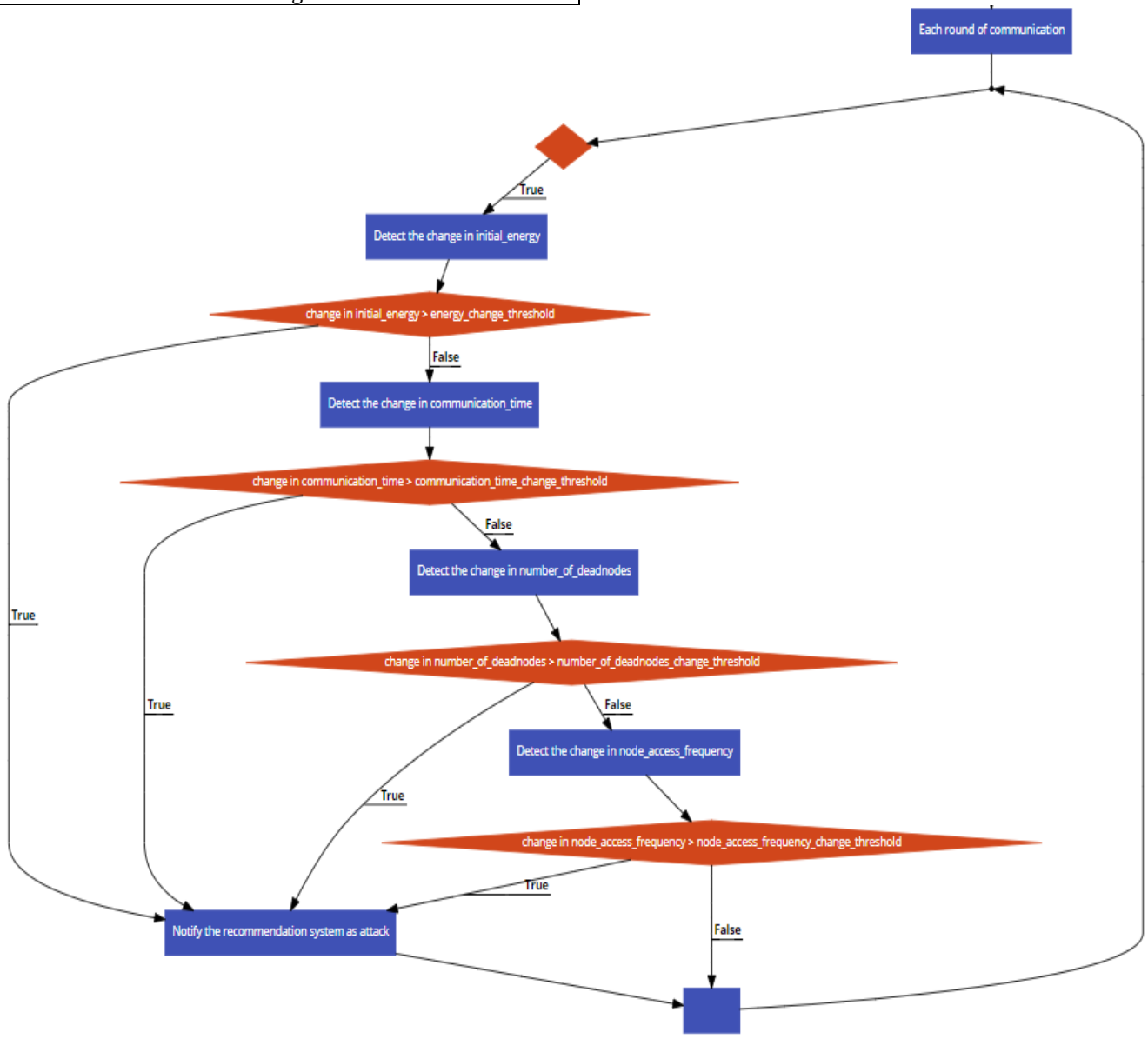

Fig.4 Attack Detection Algorithm

Further, in the light of the attacks simulated and detected, this work evaluates the results obtained from the framework.

VII. RESULTS AND DISCUSSION

In this section of the work, the work presents and discusses the results. The results are presented in this work elaborates majorly four different types of attacks and focuses on the change in parameters.

A. Parametric Observation on Energy Drain Attack

The first simulation of the attack on the proposed framework was the energy drain attack. The observations on the network parameters are furnished here [Table – VI].

TABLE-VI NETWORK PARAMETER OBSERVATION ON ENERGY DRAIN ATTACK

1	2 (Sec)	3 (Sec)	4	5	6 (Joule)	7 (Joule)
Round - 1	0.09	0.01	0	0	0.099481	0.089502
Round - 2	0.022	0.024	0	0	0.098941	0.078898
Round - 3	0.012	0.016	0	0	0.09838	0.068379
Round - 4	0.01	0.01	0	0	0.097773	0.057797
Round - 5	0.018	0.014	0	0	0.097191	0.047193
Round - 6	0.008	0.008	0	0	0.096651	0.036653
Round - 7	0.01	0.01	0	0	0.09607	0.026071
Round - 8	0.01	0.01	0	0	0.095531	0.015489
Round - 9	0.01	0.008	0	0	0.094969	0.0049281
Round - 10	0.012	0	0	20	0.094384	0

1. Rounds, 2. CommunicationTime (without Any Attack), 3.CommunicationTime (with Attack), 4.DeadNodes (without Any Attack), 5.DeadNodes (with Attack), 6.AverageEnergy (without Any Attack), 7.AverageEnergy (with Attack)

It is to be observed here that there is a drastic drop in the node energy levels. However, the communication time remains same. Hence it is natural to understand that there is no significant change in the data load on the network. But the drastic drop in the energy level denotes an attack on the network which is causing the energy drains.

The results are compared visually here [Fig.5 and Fig.6].

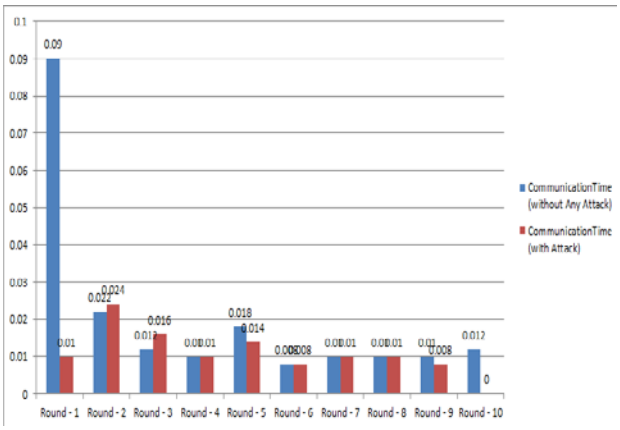

Fig.5 Communication Time

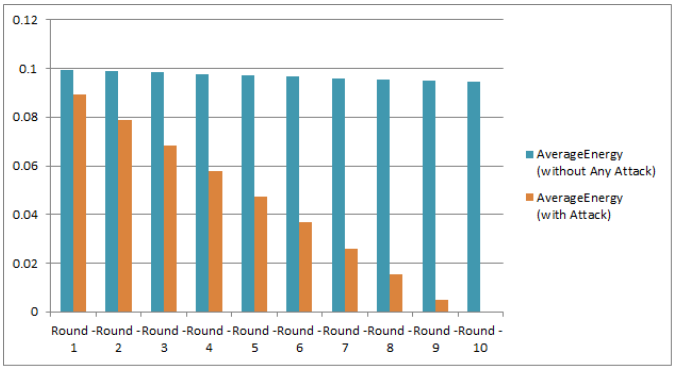

Fig.6 Energy Reduction

B. Parametric Observation on Flooding Attack

The second simulation of the attack on the proposed framework was the Flooding attack. The observations on the network parameters are furnished here [Table –VII].

TABLE-VII NETWORK PARAMETER OBSERVATION ON FLOODING ATTACK

Rounds	CommunicationTime (without Any Attack)	CommunicationTime (with Attack)
Round - 1	0.023	0.035408
Round - 2	0.005	0.0096566
Round - 3	0.003	0.0032189
Round - 4	0.003	0.0032189
Round - 5	0.005	0.0080472
Round - 6	0.002	0.0032189
Round - 7	0.002	0.0048283
Round - 8	0.002	0.0032189
Round - 9	0.002	0.0048283
Round - 10	0.001	0.0032189

It is impossible to correlate the dramatic increase in communication time for two identical set up with similar data load. This creases a suspicion of flooding attacks.

The results are compared visually here [Fig.7].

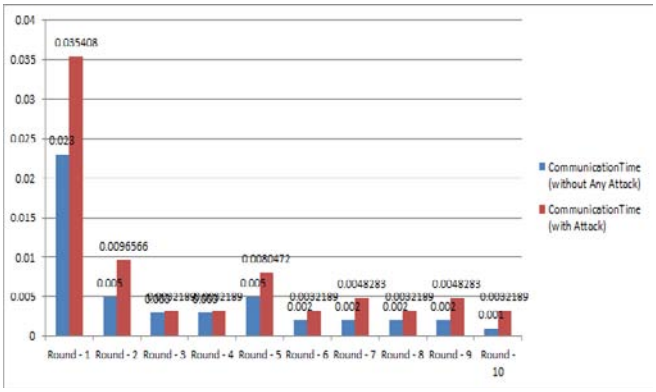

Fig.7 Increase in Communication Time

C. Parametric Observation on Interrogation Attack

The third simulation was on interrogation attack. The observations on the network parameters are furnished here [Table –VIII].

TABLE-VIII NETWORK PARAMETER OBSERVATION ON INTERROGATION ATTACK

Node Numbers	Access Density without Attack	Access Density with Attack
1	6	6
2	11	11
3	19	21
4	9	24
5	21	19
6	7	9
7	7	6
8	13	1
9	5	2
10	0	0

This is significantly observable that one specific node is being communicated frequently compared to the regular pattern of routing. Without the attack scenario, node – 2, node – 3, node – 5 and node – 8 is being communicated frequently, which is considered as regular routing pattern. During the attack scenario, the access density of node – 4 increase and crease a suspicion of interrogation attack for node – 4.

The results are visually graphically [Fig.8].

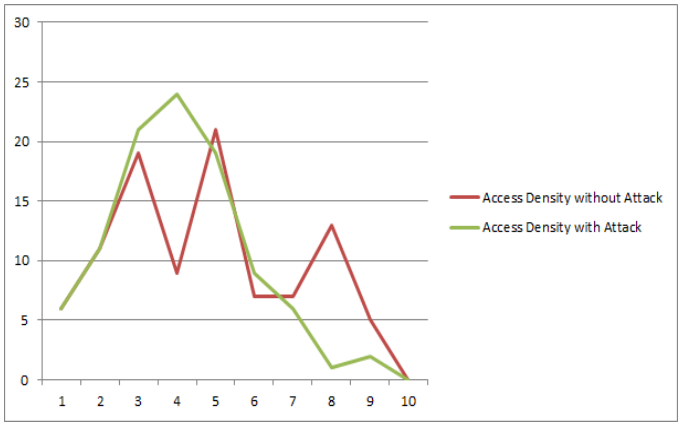

Fig.8 Access Density of the Various Nodes

D. Parametric Observation on Hello Attack

The fourth simulation was on Hello Attack. The observations on the network parameters are furnished here [Table –IX].

TABLE-IX NETWORK PARAMETER OBSERVATION ON HELLO ATTACK

1	2	3	4	5	6	7
Round - 1	0.035408	0.108	0	0	0.099481	0.07946
Round - 2	0.0096566	0.026	0	0	0.098941	0.058899
Round - 3	0.0032189	0.01	0	0	0.09838	0.038339
Round - 4	0.0032189	0.01	0	0	0.097773	0.017756
Round - 5	0.0080472	0.01	0	20	0.097191	0

1. Rounds, 2. CommunicationTime (without Any Attack), 3.CommunicationTime (with Attack), 4.DeadNodes (without Any Attack), 5.DeadNodes (with Attack), 6.AverageEnergy (without Any Attack), 7.AverageEnergy (with Attack)

The modality of this attack can be observed on communication time and energy levels for the nodes. It is to be observed that the communication time is increasing and the energy level is decreasing in the network. Also, the sudden increase in the dead node numbers can be a clear indication of having an attack situation due to high broadcasting of any message.

The results are compared visually [Fig.9,Fig.10and Fig11].

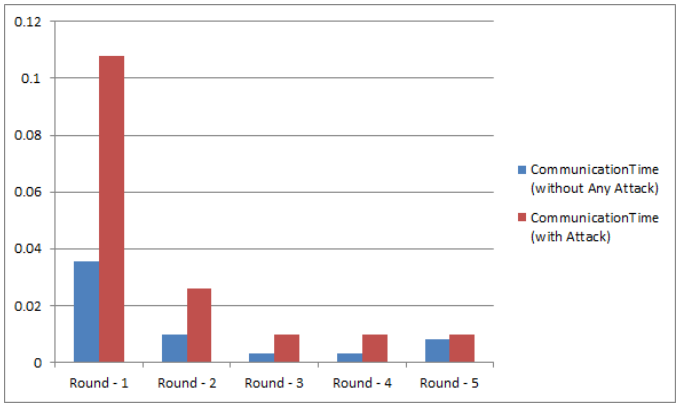

Fig.9Communication Time

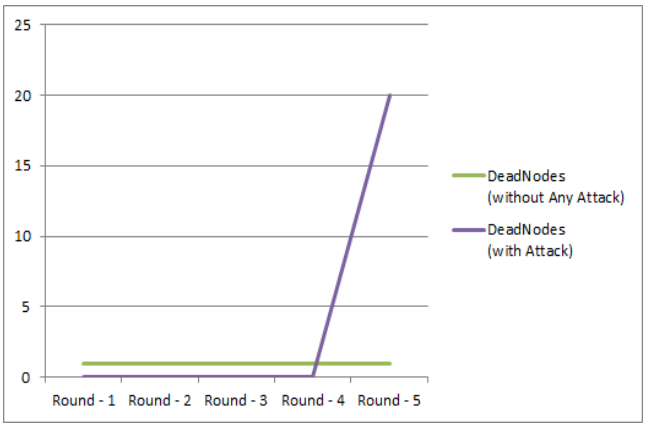

Fig.10 Dead Nodes

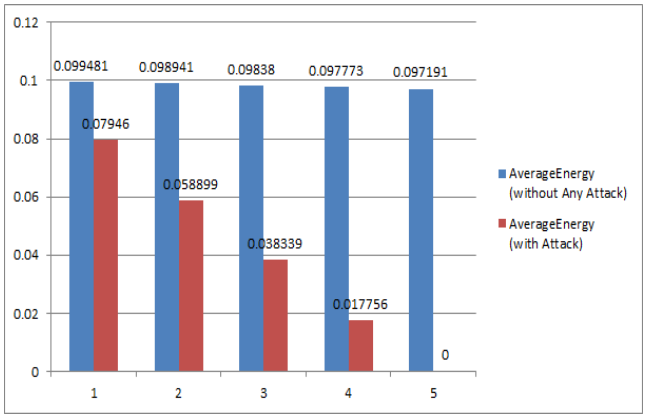

Fig.11 Energy Level

VIII. CONCLUSION

The world of wireless communication is increase along with the deployment demand for wireless sensors. The need to process data also demands the establishment of wireless sensor networks. Nevertheless, the requirements for the security for these deployed networks cannot be ignored. In order to provide proper security mechanism is the need of the current research. Thus this work analyses the types of attacks on WSN and provides a generic framework to detect the attacks based on the network parameters. Also, the lack of attack simulators motivated this work to build a significantly advanced attack simulator frameworks to observe the changes in the network parameters. This outcome will certainly help in building more network configurations with high security. The work also contributes to the counter measures during any attack, thus building a better world for wireless sensor networks.

REFERENCES

[1] Kavitha, Sridharan,"Security vulnerabilities in wireless sensor networks: A survey." Journal of Inf. Assurance and Security. 2010.

[2] Padmavathi, G.; Shanmugapriya, D. A survey of attacks, security mechanisms and challenges in wireless sensor networks. Int. J. Comput. Sci. Inf. Secur. 2009, 4, 117–125.

[3] Malik, M.Y. An outline of security in wireless sensor networks: Threats, countermeasures and implementations. Wirel. Sens. Netw. Energy Effic. Protoc. Routing Manag. 2011.

[4] Shukla, J. Bablikumari security threats and defense approaches in wireless sensor networks: An overview. IJAIEM 2013, 2, 165–175.

[5] Nguyen, H.L.; Nguyen, U.T. A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Netw. 2008, 6, 32–46.

[6] Mohanty, P.; Panigrahi, S.; Sarma, N.; Satapathy, S.S. Security issues in wireless sensor network data gathering protocols: A survey. J. Theor. Appl. Inf. Technol. 2010, 13, 14.

[7] Han, S.; Chang, E.; Gao, L.; Dillon, T. Taxonomy of Attacks onWireless Sensor Networks. In EC2ND 2005; Springer: London, UK, 2006; pp. 97–105.

[8] Lupu, T.G. Main types of attacks in wireless sensor networks. World Sci. Eng. Acad. Soc. 2009, 9, 180–185.

[9] Mohammadi, Jadidoleslamy, H. "A Comparison of Link Layer Attacks on WSN" Int. journal on applications of graph theory in wireless ad hoc networks and sensor networks.2011

[10] M. Mekni, B. Moulin, "A survey on sensor webs simulation tools", Int. Conf. on Sensor Technologies and Applications, 2008.

[11] NS-2, "The Network Simulator", 2007

[12] OMNeT+-, "www.omnetpp.org" 2012

[13] Chhimwal, P.; Rai, D.S.; Rawat, D. Comparison between different wireless sensor simulation tools. IOSR-JECE 2013, 5, 54–60.

[14] Pathan, A.K.; Monowar, M.M.; Khan, S. Simulation Technologies in Networking and Communications: Selecting the Best Tool for the Test; CRC Press: Boca Raton, FL, USA, 2014.

[15] Sarkar, N.I.; Halim, S.A. A Review of Simulation of Telecommunication Networks: Simulators, Classification, Comparison, Methodologies, and Recommendations. JSAT 2011, 2, 10–17.

[16] The Network Simulator Version 2. Available online: http://www.isi.edu/nsnam/ns/ (accessed on 2017).

[17] The NS-3 Network Simulator. Available online: http://www.nsnam.org (accessed on 2017).

[18] Contiki: The Open Source OS for the Internet of Things. Available online: http://www.contiki-os.org (accessed on 2017).

[19] Boulis, A. Demo abstract: Castalia: Revealing pitfalls in designing distributed algorithms in WSN (2007) SenSys'07. In Proceedings of the 5th ACM Conference on Embedded Networked Sensor Systems, New York, NY, USA, 4–9 November 2007.

[20] OMNeT++: Discrete Event Simulator. Available online: http://www.omnetpp.org (accessed on 2017).

[21] Zeng, X.; Bagrodia, R.; Gerla, M. GloMoSim: A library for parallel simulation of large-scale wireless networks. In Proceedings of the Twelfth Workshop on Parallel and Distributed Simulation, Banff, AB, Canada, 26–29 May 1998.

[22] Levis, P.; Lee, N. TOSSIM: A Simulator for TinyOS Networks. Tinyos Doc. 2003.

[23] Titzer, B.L.; Lee, D.K.; Palsberg, J. Avrora: Scalable sensor network simulation with precise timing. In Proceedings of the 4th international symposium on Information processing in sensor networks (IPSN '05), Piscataway, NJ, USA, 24–27 April 2005.

[24] Petrioli, C.; Petroccia, R.; Potter, J.R.; Spaccini, D. The SUNSET framework for simulation, emulation and at-sea testing of underwater wireless sensor networks. Ad Hoc Netw. 2015, 34, 224–238.

[25] Bagrodia, R.; Meyer, R. PARSEC: A Parallel Simulation Environment for Complex Systems. IEEE Comput. 1998, 31, 77–85.

[26] Peng, L.; Zeng, J. WSM: Introduction, Design and Case Study. In Proceedings of the 2007 Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007.

[27] TinyOS. Available online: http://www.tinyos.net (accessed on 2017).

[28] Sobeih, A.; Hou, J.C.; Kung, L.-C.; Li, N.; Zhang, H.; Chen,W.-P.; Tyan, H.-Y.; Lim, H. J-Sim: A Simulation and Emulation

Environment for Wireless Sensor Networks. IEEE Wirel. Commun. 2006, 13, 104–119.
[29] Dhurandher, S.; Misra, S.; Obaidat, M.; Khairwal, S. UWSim: A simulator for underwater sensor networks. Simulation 2008, 84, 327–338. Sensors , 16, 1932 26 of 27
[30] Simon, G.; Volgyesi, P.; Maroti, M.; Ledeczi, A. Simulation-based optimization of communication protocols for large-scale wireless sensor networks. IEEE Aerosp. Conf. 2003.
[31] Institude for Software Intergrated System. Jprowler. Available online: http://www.isis.vanderbilt.edu/Projects/nest/jprowler/ (accessed on 22 April 2015).
[32] Dubey, A.; Jain, V.; Kumar, A. A Survey in Energy Drain Attacks and Their Countermeasures inWireless Sensor Networks. Int. J. Eng. Res. Technol. 2014, 3. Sensors , 16, 1932 27 of 27
[33] Singh, V.P.; Jain, S.; Singhai, J. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. Int. J. Comput. Sci. Issues 2010, 7, 23–27.
[34] Abdullah, M.Y.; Hua, G.W.; Alsharabi, N.Wireless sensor networks misdirection attacker challenges and solutions. In Proceedings of the International Conference on Information and Automation, Changsha, China, 20–23 June 2008; pp. 369–373.
[35] Dubey, A.; Meena, D.; Gaur, S. A Survey in Hello Flood Attack in Wireless Sensor Networks. Int. J. Eng. Res. Technol. 2014, 3.
[36] Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. IEEE Commun. Surv. Tutor. 2011, 13, 245–257.
[37] Reindl, P.; Nygard, K.; Du, X. Defending malicious collision attacks in wireless sensor networks. In Proceedings of the IEEE/IFIP Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China, 11–13 December 2010.
[38] Ramaswamy, S. Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks. Int. Conf. Wirel. Netw. 2003, 2003, 1–7.
[39] Ding, J. Defending against path-based DoS attacks in Wireless Sensor. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05), New York, NY, USA, 7 November 2005; pp. 89–96.
[40] Zhang, Y.; Minier, M. Selective Forwarding Attacks against Data and ACK Flows in Network Coding and Countermeasures. J. Comput. Netw. Commun. 2012, 2012, 184783.

Mohammed Abdul Azeem is a Research Scholar CSE Department at JNTU,Hyderabad.He did his B.E and M.Tech in Computer Science & Engineering from Osmania University and pursuing his Ph.D in Wireless Sensor Networks from JNTU Hyderabad. His area of specialization includes Mobile Ad hoc Networks, Sensor Networks, Network Security, Algorithms and Information Security. He has published 2 papers in international journals and 2 papers presented in national conferences. He is a life member of CSI and IEI.

Khaleel Ur Rahman Khan obtained B.E. (CSE) from Osmania University in 1993, M.Tech (CS) from JNTU in 1998 followed by PhD in Computer Science from Osmania University in 2009. He is presently working as Professor in CSE & Dean (Academics) at ACE Engineering College Hyderabad. He served as Head of CSE Department at Muffakham Jah College of Engineering & Tech. Hyderabad for more than 10 years. He has taught courses like Operating Systems, Data Structures & Algorithms, Computer Networks, Programming Principles, Internet Programming, Computer Architecture and many more. He played a leading role in the preparation and execution of the process of Accreditation in both MJCET and ACE Engg. College. He delivered guest lectures and invited talks in various symposiums, workshops and Faculty development programs.His research interests include Wireless Mobile Ad Hoc Networks, Sensor Networks and Data Mining. He has more than 22 years of Teaching experience and around 10 years of Research experience. He has to his credit more than 10 papers in International journals and around 50 papers in National and International conferences. Presently there are 8 students pursuing PhD under his supervision in the area of Ad Hoc Networks and Data Mining