ISSN No:-2456 –2165

Defending Against Path-Based Denial of Service Attack in Wireless Sensor Network

Kavita S. Yadav
Second Year Student of M. E. EXTC
ARMITE College
Asangaon, Mumbai

Mujib Tamboli
Department of Electronics and Telecommunication
Engineering, AIKTC college.
New Panvel, India

Abstract—Wireless sensor network (WNS) are greatly differs from the traditional network architecture due to its energetic environment and limiting constraints and its calculated wireless applications. Because of these differences, security has become important issue. The path-based denial of service (PDoS) attacks harm the network services and has resulted in serious damage in the resource constrained WSNs. In a PDoS attack, an attacker can overwhelm sensor node and cluster head node to flood packets along the routing path so that intermediate node must keep active mode and exhaust the energy. In this paper we propose new creative approaches that work on the base station to detect mischievous attitudes. The proposed method is combined with triple exponential smoothing and Markov chain, so that it makes the finding results more accurate. At the same time Energy efficient, fault tolerance, scalability and connectivity and reliability are major challenges in wireless sensor network. Therefore, Energy efficient two level distributed clustering (EE-TLDC) Scheme is proposed with two level cluster head. The proposed scheme efficiently detects the malicious node and reduces the energy consumption in the network. Simulation shows that proposed scheme prolongs the stability period and reduces energy consumption in the network.

Keywords:-Wireless Sensor Network (WSNs), Path-Based Denial of service (PDoS), Energy Efficient Two Level Distributed Clustering (EE-TLDC).

I. INTRODUCTION

A. An Overview on WNS

Wireless sensor network (WSN) is the group of homogenous, self-organized nodes called sensor nodes. These nodes have the capabilities of sensing, processing and communication of data with each other wirelessly using radio frequency channel. The main task of sensor networks is to sense the events, collect data and send it to their requested destination. Many of the features of these networks make them different from the traditional wired and wireless distributed systems. Traditional wired or wireless networks have enough resources like unlimited power, memory, fixed network topologies, enough communication range and computational capabilities. These attributes make the traditional networks able to meet the communication demands. On the other hand, the sensor nodes are not only low power electronic devices but also deployed in remote areas where power resources are limited. In additions they are subject to open wireless communication. Since the resources of the sensor nodes are severely constrained and may be deployed in an unattended or even hostile environment, WSNs can be easily attacked by denial-of-service (DoS) attacks, which cause information loss along with large energy expenditure [1]. In DoS attack, an attacker may compromise a sensor node to access all data stored on the node and perform insider attacks [2]. The applications of the WSNs are usually environment monitoring, home-care surveillance, habitat monitoring, military surveillance, and so forth.

B. Security Issues in WSN

Security is one of the important concern of any communication network. Many attacks have been reported over the last several years. Most of them, however, target wired networks as compared to wireless. Now wireless networks have recently been gaining popularity as world is going towards wireless technology. Nowadays, with progress in wireless technology, the wireless network is becoming more affordable and easier to build. Many metropolitan areas deploy public WMANs for people to use freely. Moreover, the prevalence of WLANs as the basic edge access solution to the Internet is rapidly becoming the reality. However, wireless networks are vulnerable with an important security flaw; they are much easier to attack than any wired network. The shared and easy to access medium is undoubtedly the biggest advantage of wireless networks, while in particular, it makes it extremely easy for an attacker to launch an attack. Denial of Service Attack (DoS) has increased the importance of this protection as an accessibility view in the context of security, not just the resolution of confidentiality and integrity. Attackers use DoS in many different ways, including extortion threats, obfuscation, hacktivism and even friendly fire.

C. Types of DoS Attacks in WSN

There are so many types of denial of service attacks. Each layer is vulnerable to different kind of DoS attack and has different options for its defense. Classification is as follows.

ISSN No:-2456 –2165

PROTOCOL LAYER	ATTACKS	DEFENSES
Physical	1. Jamming	1.Detect and sleep Route around jammed regions
	2. Node Tampering or Destruction	2.Hide or camouflage nodes Tamper-proof packaging
Link/ MAC	1. Interrogation	1.Authentication and anti-replay protection
	2. Denial of Sleep	2.Authentication and anti-replay protection
Network	1.Spoofing, replaying, or altering routing control traffic	1.Authentication and anti-replay protection
Transport	1. SYN Flood	1.SYN Cookies
	2.Desynchronization attack	2.Packet Authentication
Application	1. Overwhelming sensors	1.Sensor tuning and Data aggregation
	2. Path-Based DoS Attack	2.Authentication and anti-replay protection

Table 1: Types of Denial of Denial of Service Attacks.

So, there is numerous denial of service attack on network and protocol layer. Out of these attacks path-based denial of service attack is seeming to be most dangerous to the network.

D. Special form of attack in WSN : Path-Based Denial of Service Attack (PDoS).

Different types of DoS attacks in different layers have been discussed in [3], and some countermeasures to defend against the mare proposed. But in the numerous DoS attack, there is a special form of attack called the path-based DoS (PDoS). The PDoS was first pointed out by Deng et al. [4] in 2005.They described that a PDoS attack begins with the sensor nodes and cluster heads (CHs), compromised of an adversary that floods numerous packets through multi hop communication to base station or sink node along the established routing path. As a result, the intermediate nodes in the routing path have to keep active mode and forward the packets so that they cannot return to sleep mode normally. Generally speaking, the PDoS targets the intermediate nodes within the routing path to exhaust their energy. Figure 1 has shown how the PDoS launches the attack.

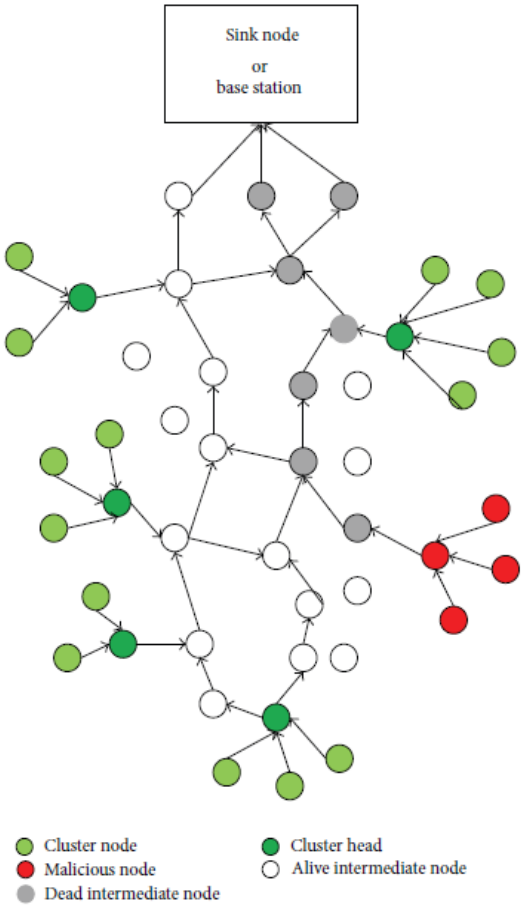

Figure 1: Network attacked by PDoS.

II. LITERATURE SURVEY

In order to defend against a PDoS attack, the intermediate nodes should be able to detect the malicious packets and then reject them. Deng et al. pointed out that two ways generally are adopted. One is to have the source node establish a separate shared key with other sensor nodes in the routing path. The other is rate control, which limits the number of packets an intermediate node can forward per second. But the highly restricted packet size and nodes at different locations need to forward different numbers of packets per second making these two ways hard to directly defend the PDoS attack. However, several schemes have been proposed to defend the PDoS attack, which are also based on these two ways. Deng et al. [4] proposed a lightweight secure mechanism, which uses one-way hash chain to defend against PDoS attacks on intermediate nodes in a multi hop end-to-end data path in WSNs. Perrig et al. [5] proposed a loosely time synchronous mechanism called the timed efficient stream loss-tolerant authentication (TESLA) broadcast authentication protocol, and it comes with the denial-of-service attacks. However, the time asynchronous problem causes the sensor node to be unverifiable whether the messages are valid or not before the trusted party releases the trapdoor key. Cheng et al. [9] proposed an efficient QoS-aware GOR (EQGOR) algorithm. To some extent, this algorithm can resist DoS attack and has a very low time complexity, which is specifically tailored for the resource limitation of sensor

devices. The bloom filter of the statistical en-route filtering (SEF) scheme was proposed by Ye et al. [7] and it is used to reduce the MACs size and ensure their security.

Hence, most previous schemes need intermediate nodes to verify the truthfulness of each data that they received and decide to forward or drop. This wastes the energy consumption of the intermediate nodes. Moreover, the cluster heads have to increase the bits in packet for verification, and this extra overhead also consumes the energy of intermediate nodes when the packets are forwarded. Compared with the previous papers, our mechanism is a novel solution to defend the PDoS and achieves the energy conservation for the intermediate nodes, and hence the network lifetime becomes longer.

III. PROPOSED SYSTEM

In this paper we propose new creative approaches that work on the base station to detect mischievous attitudes. The proposed method, which combines triple exponential smoothing and Markov chain for detecting the attack behavior. This method is completely different from other detecting algorithms. The proposed method is operated on the base station or sink node rather than in the intermediate nodes, because they have more power and energy. It brings great benefit in conserving energy of the intermediate nodes. At the same time we are using Energy-Efficient two level distributed clustering protocol. At the first level clustering the data from SN to primary CH, at second level data is transmitted from primary CH to Through direct transmission from CH to BS whoever is nearest. So, it results in prolong stability period and reduces energy consumption in the network.

IV. SYSTEM ARCHITECTURE

A. Assumption:

In this section, we make two assumptions for network model and adversary Model, for ease of simulation of the methodology for Defending against path-based denial of service attack in WSN.

B. Adversary Model:

The adversary(Attacker) controls the compromised nodes and accesses all the secret data to perform insider attacks. The compromised CH floods numerous replayed and false data. Herein, we mainly consider a single point of attack which is able to damage the network for the CHs have more energy.

C. Attack Behavior Detection Algorithm

Without loss of generality, the base station has better capability on energy and computation. Due to the reduced energy of the intermediate nodes, we adopt the base station to validate that the network has been attacked by PDoS or not. For this process we adopt triple exponential smoothing of the time series forecasting and the Markov model based on the nodes energy.

V. SYSTEM ALGORITHM AND FLOWCHART

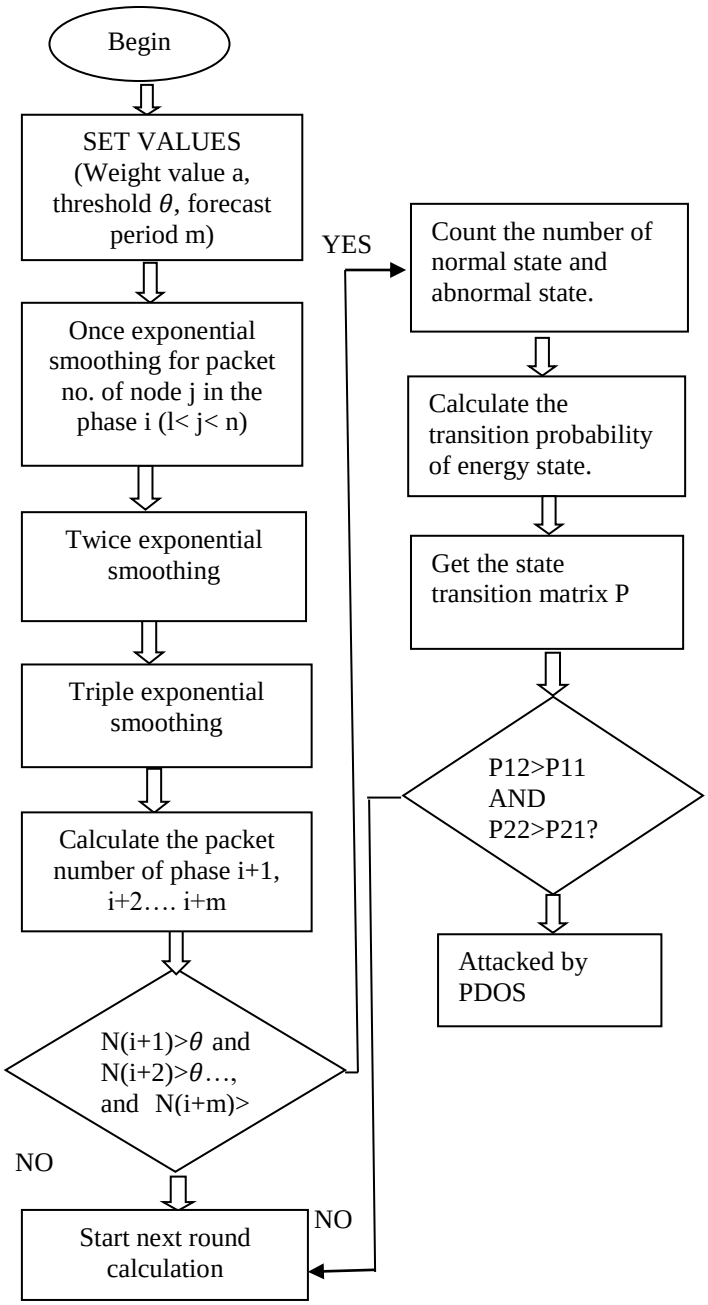

Figure 2: The Flow Diagram of Attack Behavior Detection Algorithm

VI. WORKING PRINCIPLE

Firstly, the base station adopts the method of triple exponential smoothing to forecast the number of the packets at phases i + 1, i + 2, . . ., i + m, which are sent by the same node and then compares these forecasted values with the threshold θ. If all values are larger than θ, we believe that the network has been attacked by abnormal packets, but maybe not the PDoS attack. Third, base station uses the method of prediction model about the node energy status based on Markov chain. If the energy state of the node in the next phase is abnormal, we may believe the node is malicious. At last, the judgment results are obtained. Only these two conditions are recognized as attacked

by PDoS attack, the energy state of the node in next phase is abnormal, and the forecasting values of the packets which are larger thanθ are confirmed at the same time.

Phase 60 sec	IP1	IP2	IP3	……..	IPn
Phase 1	107	95	85	……..	130
Phase 2	130	100	89	……..	128
Phase 3	120	104	97	……..	110
.	.	.	.	……..	.
.	.	.	.	……..	.
Phase i	125	115	100	……..	103
.	.	.	.	……..	
.	.	.	.	……..	

Table 2: Packet Number Received By Base Station In Each Phase

The formula of once and twice exponential smoothing are shown as follows:

$$S_t^{(1)} = \alpha y_t + (1-\alpha)S_{t-1}^{(1)} \quad \ldots\ldots\ldots\ldots (1)$$

$$S_t^{(2)} = \alpha S_t^{(1)} + (1-\alpha)S_{t-1}^{(2)} \quad \ldots\ldots\ldots (2)$$

Then, according to the following, we continue to get the third exponential smoothing value:

$$S_t^{(3)} = \alpha S_t^{(2)} + (1-\alpha)S_{t-1}^{(3)} \quad \ldots\ldots\ldots\ldots\ldots (3)$$

$$Y_{t+m} = a_t + b_t m + c_t m^2 \quad \ldots\ldots\ldots\ldots (4)$$

Where Y_{t+m} its mathematical model of triple exponential smoothing.
m: forecast period, t + m: prediction of phase
The coefficients at, bt and ct are all smoothing factors.

A. Prediction Model of the Node Status Based on Markov Chain.

By monitoring the nodes energy consumption in each phase, we mark the status of nodes in different time. Therefore, we can get the transfer probability of different status. Based on the transfer probability, we recall a Markov chain model to predict the node energy status in next phase.

The energy of each node is divided into five levels, such as 100%, 75%, 50%, 25%, and 0%. Note that the percentage of energy is based on the residual energy of nodes. The monitor time is ΔT; it means the node monitors the energy information every ΔT = 1 sec. If the transfer hop of different energy status is larger than one, we regard this node as abnormal. For example, node A detects that the energy is 100% at ΔT1, and the energy is 50%, 25%, or 0 at Δ□2; we recognize node A as abnormal node.

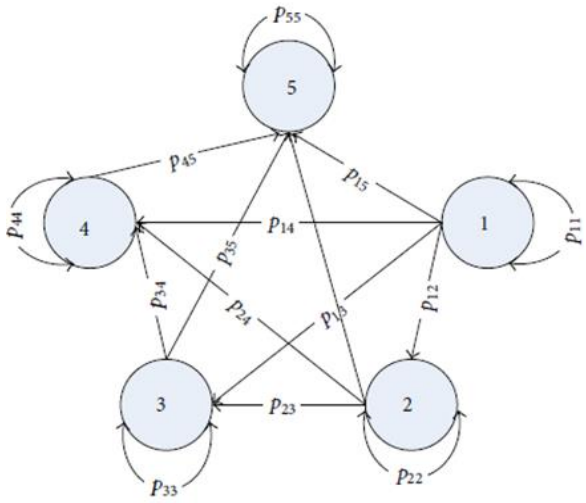

Figure 3: The Transition Diagram of Markov State

$$\begin{pmatrix} p_{11} & p_{12} & p_{13} & p_{14} & p_{15} \\ p_{21} & p_{22} & p_{23} & p_{24} & p_{25} \\ p_{31} & p_{32} & p_{33} & p_{34} & p_{35} \\ p_{41} & p_{42} & p_{43} & p_{44} & p_{45} \\ p_{51} & p_{52} & p_{53} & p_{54} & p_{55} \end{pmatrix}.$$

In the following content, we use an example to elaborate and illustrate how to forecast the energy state of the node. In the phase i, base station detects the energy information of each node per one second and records the state as normal or abnormal. Therefore, there are 60 states, which are 25 normal states and 35 abnormal states.

- The number of state transitions from normal state to normal state is 11.
- The number of state transitions from normal state to abnormal state is 15.
- The number of state transitions from abnormal state to normal states is 12.
- The number of state transitions from abnormal state to abnormal state is 21.

Then, we make the "character 1" to present the normal state, and "character 2" presents the abnormal state. Hence, we can conclude the state as follows.

$$P_{11} = \frac{11}{26},\ P_{12} = \frac{15}{26},\ P_{21} = \frac{12}{33},\ P_{22} = \frac{21}{33} \ldots (5)$$

The state transition matrix of the Markov chain is

$$P = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix} = \begin{pmatrix} 0.423 & 0.577 \\ 0.364 & 0.636 \end{pmatrix} \ldots\ldots (6)$$

From the matrix of p, we find that $P_{12} > p_{11}$, which means the energy state of the node is normal at phase...i. But the probability that the energy state is abnormal at phase $i+1$ is

larger than normal and $P_{22} > P_{21}$ which means that the energy state of the node is abnormal at phase i, but the probability that the energy state is also abnormal at phase $i+1$ is larger than normal. Accordingly, we summarize that no matter what the energy state of the node is in the current phase, the probability of the energy state is abnormal and is larger than normal in the next phase. And we can judge that this node could be malicious.

Combining these two methods described above, we are able to judge exactly whether the network has been attacked by PDoS.

B. Step for Defending Against PDOS Attack:

With the help of attack behavior detection algorithm, it would be easy to find whether the network has been attacked and locate where the attacker launched an attack accurately. But just finding attack behavior is not our only goal because the network is still resistless to the PDoS attack. Therefore, we use two routing protocol. i.e. AODV and Energy efficient two level Distributed clustering protocol (EE-TLDC) to prolongs the stability period and reduces energy consumption in network.

A. AODV

Ad-hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks and is capable of both unicast and multicast routing. It sets the path between nodes only as desired by source nodes. It maintains these routes as long as they are required by the source nodes. Also, the AODV protocol forms tree structure which connects multiple group members. The trees are collection of the group members, and the nodes need to connect the members. AODV uses sequence numbers to ensure the unique id or smoothness of routes.

a). Energy Efficient Two Level Distributed Clustering Protocol.

Step1: In the proposed technique, the two-level hierarchy is used to transmit data from SNs to base station to save transmission costs. At first level, clustering is used for routing the data from SNs to primary CH. At second level, data is transmitted from the primary CH to BS through the secondary CHs (elected from primary CHs) or through direct transmission from CH to BS whichever is nearest. In order to reduce the need of global knowledge of sensor nodes ideal value of network lifetime and average energy consumption in round is estimated as proposed in DEEC [7]. Network Design: In real scenario, WSNs may have different energy levels of SNs. Network operations or re-energization of network creates heterogeneous network with large range of energy level SNs. So, network is designed with three levels of heterogeneity containing normal, advanced and super sensor nodes with different energy level. Super SNs are considered as M2 fraction of total N number of SNs and having ù times more energy than normal SNs. Advanced SNs are M1 fraction of total SNs and having Į times more energy than normal SNs and others are normal SNs. So, network with total N sensor nodes (in M*M sensor field) is having N*M1*M2 super sensor nodes, N*M1*(1-M2) advanced nodes and N*(1-M1) normal nodes. E_0 is initial energy of the normal node. E_0* (1+b) is energy of each super node and E_0* (1+a) is energy of each advanced node. Presence of heterogeneity increase total energy in the network. Total initial energy of the network is sum of initial energies of SNs, can be is computed as:

E_{Total} = N*M1*M2(1+b) E_0 +N*M1(1-M2) (1+a) E_0 +N(1-M1) E_0 =N*E_0(1+M1 (a+M2 (-a+ b))) …… (1)

So, total energy of network is increased by (1+M1 (a+M2 (-a+ b))). Virtually network has N* (1+M1 (a+M2 (-a+ b))) number of SN with equal energy. For simulation it is assumed that sensor nodes are randomly deployed which are stationary or micro-mobile. Base station is far away from sensor field. All SNs are sensing the surroundings at fixed rate and thus always have data for transmitting to BS. Fixed size packets are transmitted throughout the network. The proposed technique follows the steps below.

Step1: Estimating ideal value of network lifetime and average energy consumption Average energy is ideal value that each node should possess in current round to keep the network alive to the greater extent. Energy of sensor network and SNs is uniformly distributed in such ideal situation. Average energy is used as reference energy and actual energy fluctuates around it. Average energy of rth round can be estimated as

$$E_{avg}(r) = \frac{1}{N} E_{total}\left(1 - \frac{r}{R}\right) \quad \text{…… (2)}$$

Where R is ideal value of network lifetime, calculated as given

$$R = \frac{E_{Total}}{E_{Round}} \quad \text{……... (3)}$$

Due to the presence of heterogeneity R is taken 1.5 times of calculated value. Since average energy of network will be too large at the end from (2) and some sensor nodes will not die finally [7].

E_{Total} is total energy of network as calculated in (1) and E_{Round} is energy dissipated by network in a round. For calculation of energy dissipation in network, first order radio model is used [2, 6, and 7]. Energy expenditure for transmitting ETX, L-bit message over distance d is calculated as

$$E_{TX}(L, D) = \begin{cases} LE_{elec} + LE_{fs}\, d^2 \\ LE_{elec} + LE_{mp} d^4 \end{cases} \quad \text{…. (4)}$$

Elect is energy dissipation while receiving or transmitting a single bit data with distance d. L denotes number of data bits in a single packet. Efs and Emp are free space and multi-path fading models. If distance between sender and receiver is less than threshold distance does then free space model (d2 power loss) otherwise multi-path fading model (d4 power loss) is considered.

Step2: First level Clustering Primary CHs are chosen in this level of clustering. Cluster head selection depends on the average probability of each SN which is calculated with residual energy of sensor node and average energy of network. An Epoch is number of rounds in which each SN becomes CH at least once [6]. The value of Epoch for being cluster head for SNs is different according to initial and residual energy of node as in [7].

For cluster head selection, algorithm is broken in rounds, as in LEACH [2]. Where a round is time interval in which all sensor nodes transmit to their CH [6]. In each round, algorithm undergoes two phases: Setup phase that includes cluster head selection and steady state phase that includes transmission. In setup phase, SNs decide whether to become CH or not based on threshold T (S_i), calculated by average probability Pi and epoch r mod ($\frac{1}{P_i}$) of each SN si, which belongs to set G, as supposed in [7]. A random number is selected by each sensor node in range [0,1]. If chosen number is less than threshold, the SN becomes cluster head for current round, r. G is set of SNs which have not been CH in current epoch.

$$T(S_i) = \begin{cases} \frac{P_i}{1-P_i(r \bmod \left(\frac{1}{P_i}\right))}, & If\ S_i \in G \\ 0 & Otherwise \end{cases} \quad ...(5)$$

In homogeneous network all sensor nodes are identical in terms of their initial energy. Each node is having equal probability to be cluster head. P_{opt} is optimal probability for SN to be CH [2]. In heterogeneous networks SNs have different initial energy. For two-level heterogeneous SEP protocol, normal and advanced nodes have different probabilities to be CH based on their initial energies. In DEEC, average probability for two-level heterogeneous network was proposed. In this paper, average probability calculated in DEEC is extended and proposed for three-level heterogeneous network is calculated. Average probability P_i of each sensor node is calculated based on residual energy $E_i(r)$ of node and average energy of network E_{avg} for current round [7]. P_{opt} is reference value of P_i and is different for three energy level/heterogeneous sensor nodes.

CH nodes are responsible for collection, aggregation and transmission of data toward BS. Optimal number of cluster heads is given as k. The amount of consumed energy for all the clusters is same. For uniform distribution of SNs in the clusters, each cluster should have N/k sensor nodes.

Energy dissipated by cluster head node, ECH for receiving data from associated SNs, data fusion and transmitting to Secondary cluster head (SCH) or BS whichever is near is given.

$$E_{CH} = L\left[\left(\frac{N}{K} - 1\right) E_{elec} + \frac{N}{K} E_{DA} + E_{elec} + E_{fs} d^2_{toSCH}\right] \quad .. (6)$$

First part of equation shows the energy dissipated in receiving message from associated SNs excluding itself. EDA is energy used for fusion of itself and received data. Remaining part of equation is energy dissipated for data transmission to secondary cluster head as described in (4). d_{toSCH} is distance from CH to associated secondary CH. Energy dissipation is calculated as proposed in SEP but receiver can be SCH or BS in proposed work. Equation (7) can be simplified as follows.

$$E_{CH} = L\left[\left(\frac{N}{K}\right) E_{elec} + \frac{N}{K} E_{DA} + E_{fs} d^2_{toSCH}\right] \quad ....(7)$$

Energy dissipation of non-cluster head node E_{non-CH} include energy used in transmitting the data to their associated cluster head is given by [6]:

$$E_{non-CH} = L\left[E_{elec} + E_{fs} d^2_{toCH}\right] ..... (8)$$

d_{toSCH} is distance between the sensor node and CH.

Step3: Second Level Clustering According to first order energy model energy dissipation increases with distance. So, if distance from CH to BS can be reduced for some CHs, network energy can be saved. Base station is considered away from network. Set of CHs is chosen as Secondary Cluster Heads (SCHs) from primary CHs, elected during Step 2. Instead of all CHs, only few SCHs transmit BS and undergo transmission losses. Selection of Secondary CHs from Primary CH is done on the basis of distance from sink. If distance between primary CH and base station is less than the average distance d_{avg} it is chosen as secondary cluster head. d_{avg} is average distance of all sensor nodes from base station, can be computed as given below.

$$d_{avg} = \frac{1}{N}\sum_{i=1}^{N} d(i) ..... (9)$$

Number of secondary cluster heads can't exceed half of number of chosen primary cluster heads. Therefore, half or less than half cluster heads will only transmit to BS that have less transmission distance. Energy dissipation by secondary cluster head ESCH, contains energy consumption while receiving data from associated cluster heads, aggregating received data with own data and transmitting to BS with distance d_{toBS} ESCH can be calculated as.

$$E_{CH} = L\left[E_{elec} + E_{DA} + E_{elec} + E_{fs} d^2_{toBS}\right] \quad .... (10)$$

Primary/Non-Secondary CH transmit aggregated data toward associated Secondary CH. Energy dissipation of no secondary CH nodes E_{non-CH} will be while transmitting data to secondary CH for distance is given below:

$$E_{non-SCH} = L\left[E_{elec} + E_{fs} d^2_{toSCH}\right] ... (11)$$

ISSN No:-2456 –2165

VII. SOFTWARE SIMULATION

The simulation is conducted on MATLAB simulator, and used parameters are shown.

SIMULATION PARAMETER	VALUE
Node number	100
Topology	Fixed
Interference type	Physical/wireless Phy
Base Station	1
Packet size	4000(bit)
Cluster Head	Not fixed
Advance node	Not Fixed
Super node	Not fixed
Initial energy	0.12 joules
DEEC Parameter	Variable
Threshold Value	0.7
M	1
Round	Fixed

Table 3. Simulation parameter

VIII. SIMULATION RESULT

A. Two level heterogeneous clustering Network model.

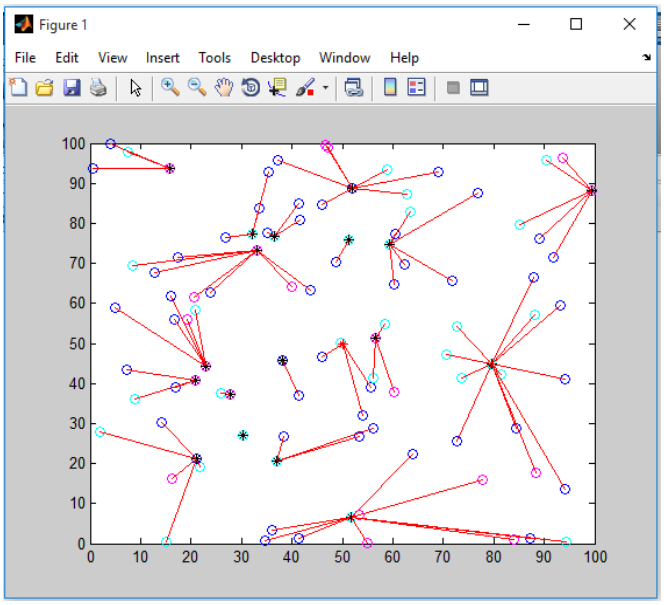

Figure 4: Simulation Snapshot of Two Level Heterogeneous Clustering Network Model.

In this network model, any of the node act as base station or sink node having highest energy among the other node. Then after each round of transmission of data any of the node can be converted into cluster head, advance node and super node based on their remaining energy, and distance to the base station, so that disimpassion of energy should be less while transmitting data to the base station.

B. Detection of Malicious Node in the Two-Level Heterogeneous Clustering Model.

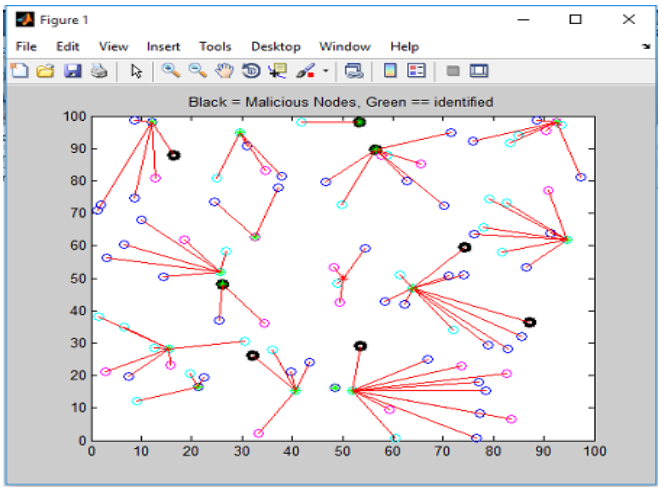

Figure 5: Simulation Snapshot of Detection of Malicious

- So, we can see that here 8 nodes are identified as malicious node.
- To confirm that this attack is path base denial of service attack (PDOS) we use Triple exponential smoothing and markov chain, by this we confirm that attack is path-based denial of service attack.
- So, Detection attack is not the ultimate goal so we tried to defend against path-based denial of service attack by using AODV Protocol and EE-TLDC Scheme. Which increase the stability of sensor network and Reduces the energy consumption of each node while data transfer from node to base station.

C. Detecting against path-based denial of service attack in the two-level heterogeneous clustering model.
Number of Malicious node=8

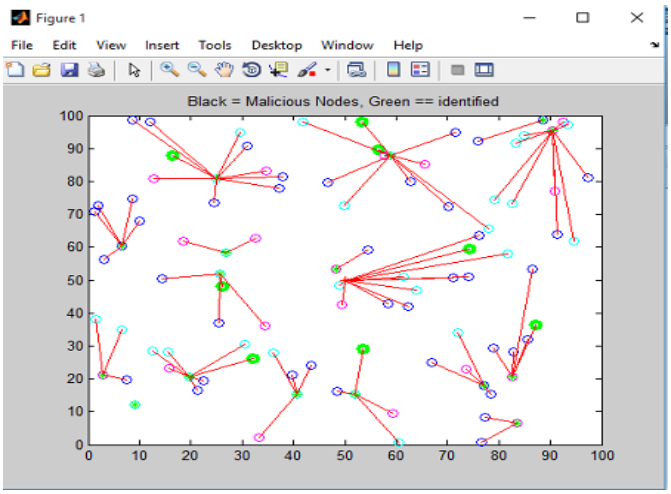

Figure 6: Simulation Snapshot of Defending Against Malicious Node.

So after identifying the malicious node we stop the data transmission from that nodes and try to protect the network

from this malicious data to flow through network.We also improve the stability of nodes in the network and energy consumption of each node in the network while transferring the data with the EE-TDLC Scheme.We can see the performance of the network with Graph of Congestion level, Energy consumption in the network, Number of packet transmission from Cluster Head to Base station, formation of cluster head and alive nodes in of the network Without EE-TDLC scheme and with EE-TDLC Scheme.

IX. COMPARATIVE GRAPH

Case 1: Network performance with PDOS Attack without EE-TDLC

Number of malicious node: 08

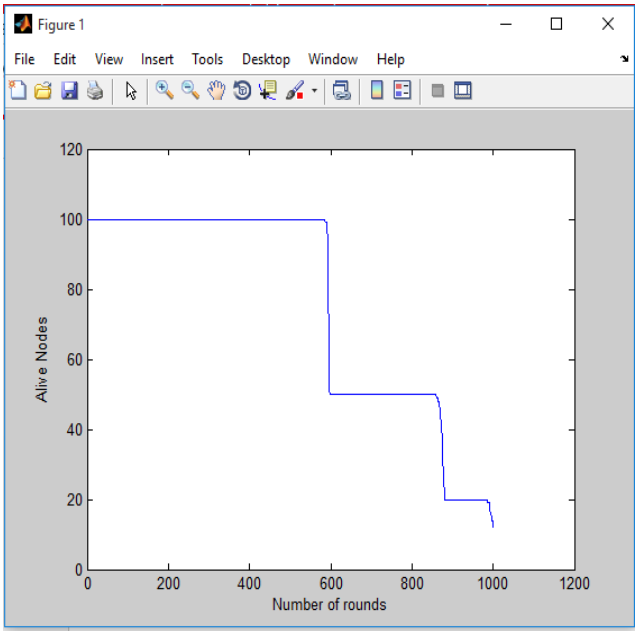

Figure 7: Alive Node Vs Number of Rounds.

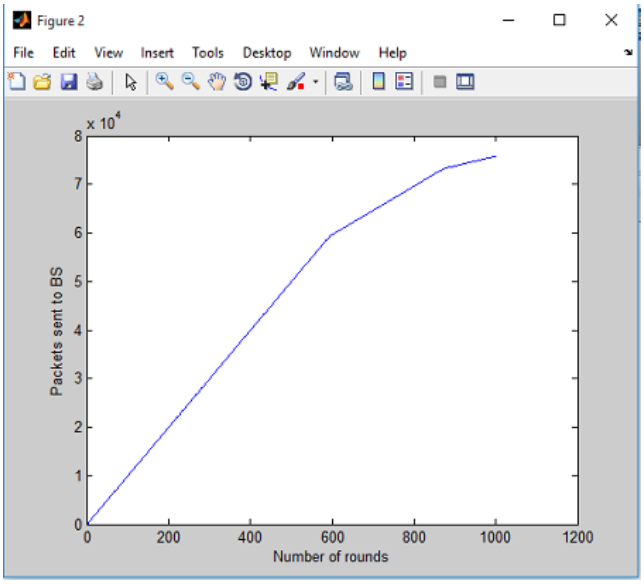

Figure 8: Packet Sent to BS Vs Number of Rounds

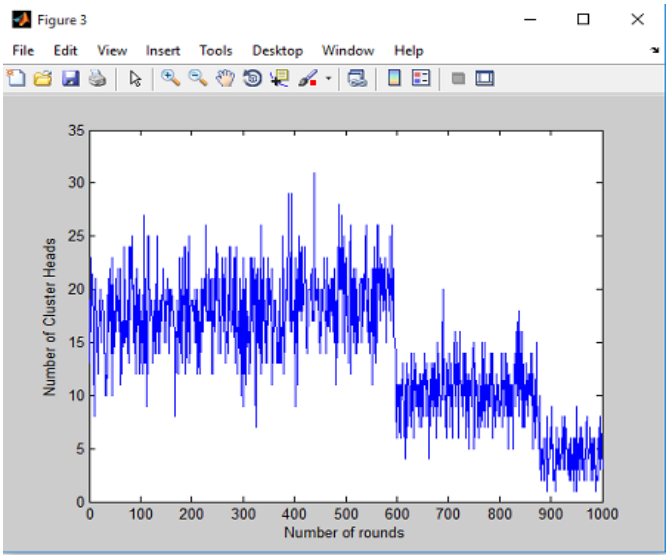

Figure 9: Number of Cluster Head Vs Number of Rounds

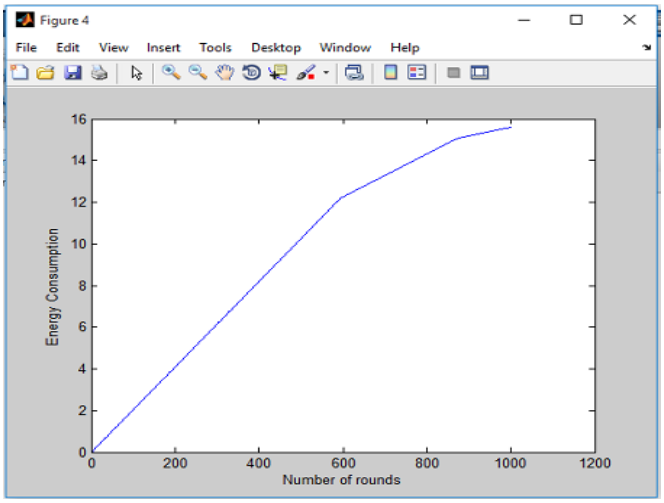

Figure 10: Energy Consumption Vs Number of Rounds

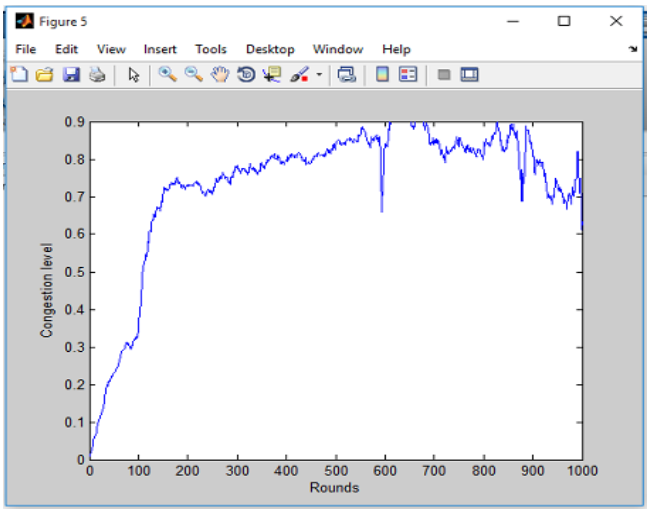

Figure 11: Congestion level Vs Number of Rounds

Case 2: Network performance with Proposed Scheme.
Number of malicious node: 08

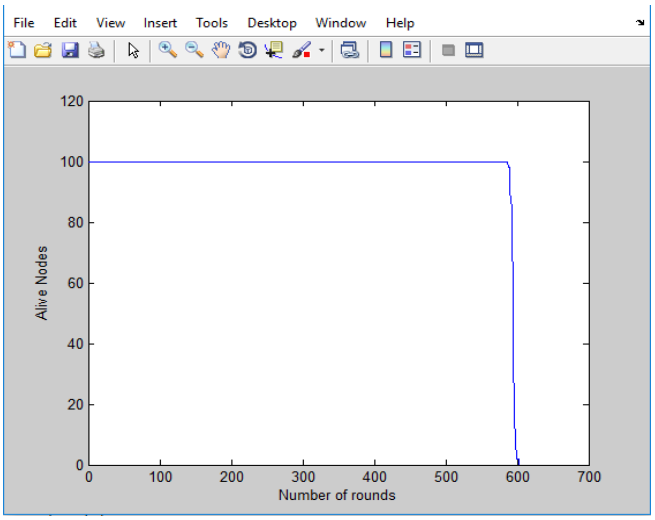

Figure 12: Alive Node Vs Number of Rounds with EE-TDLC scheme.

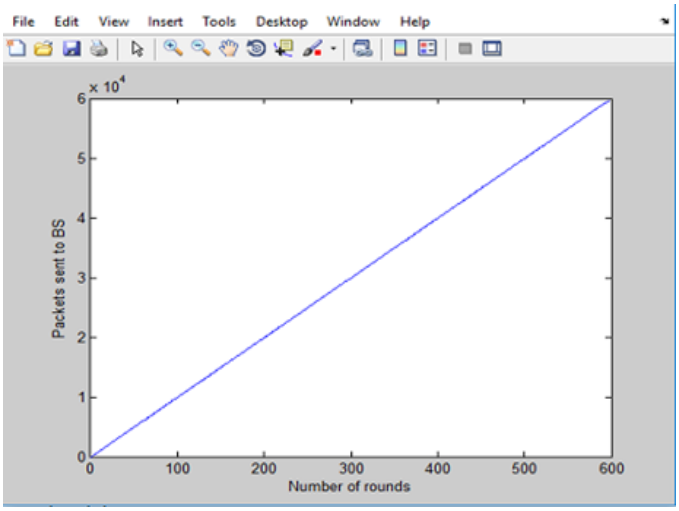

Figure 13: Packet Sent to BS Vs Number of rounds with EE-TDLC scheme

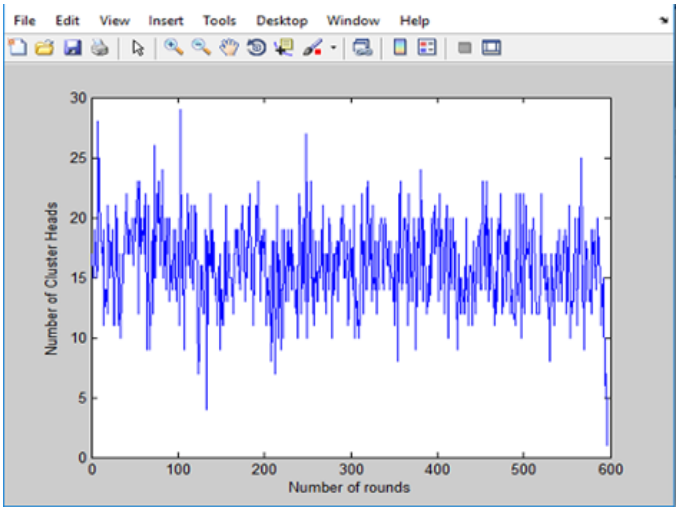

Figure 14: Number of Cluster Head Vs Number of rounds with EE-TDLC scheme

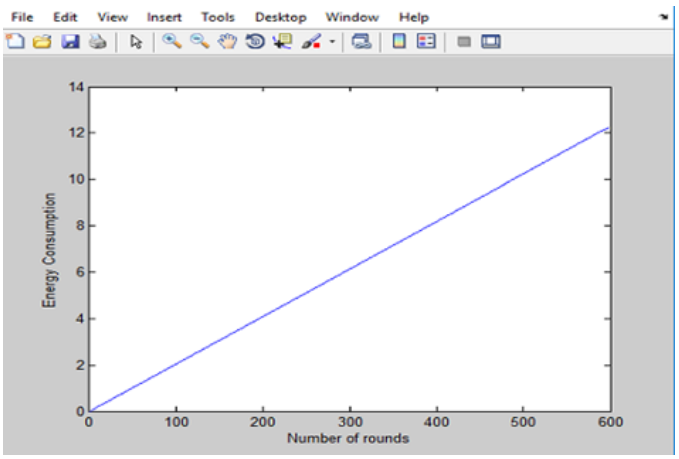

Figure 15: Energy consumption Vs Number of rounds with EE-TDLC scheme.

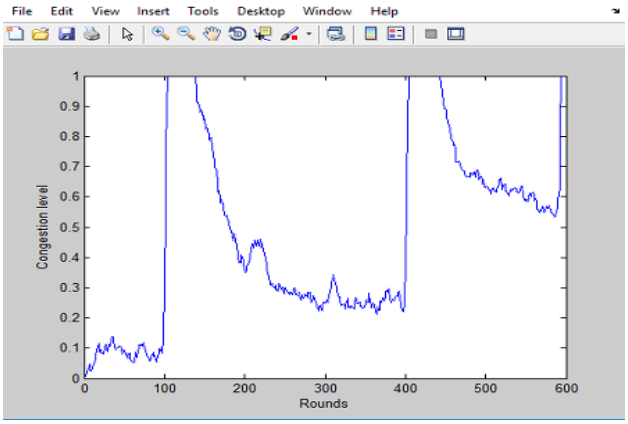

Figure 16: Congestion level Vs Number of rounds with EE-TDLC Scheme.

1) *Network Lifetime (Live Nodes):* Cluster heads are not only responsible for communicating with BS, but also receiving and aggregating that data. CHs are selected randomly. There is a possibility that distance between the selected CH and BS can be long. This will cause high energy consumption of CH and leads to smaller lifetime of CH. To avoid this problem, secondary CHs are selected in EE-TLDC. It is observed that EE-TLDC outperforms DEEC in terms of stability period. As secondary CH saves transmission distance for primary CHs so energy of SNs is saved. During instability period, more number of SNs in EE-TLDC remains alive per round.

2) Packet Transfer to BS: with the proposed scheme packet transfer to base station is efficiently increased.

3.) Cluster Head Formation: Cluster heads are formed in DEEC and EE-TLDC for nearly same number of rounds but the numbers of cluster heads per round are increased in EETLDC as compared to DEEC. Fig. 5 shows the CH formation in DEEC and EE-TLDC and indicates that numbers of CHs in EE-TLDC are higher.

4) Energy Consumption: Energy dissipated in each round is reduced in proposed technique using secondary cluster heads. Total energy of network in considered case is nearly 110

ISSN No:-2456 –2165

Joules. Fig.3 shows the energy consumption curve and it shows that energy consumption per round in EE-TLDC.

5) Congestion Level: We can see in the graph that due to attack there are increase in congestions level due to flooding of malicious packet. Which is be reduced to great extent with the help of this proposed Scheme.

X. CONCLUSION AND FUTURE WORK

In this paper, we propose a novel solution to defend the PDoS attack. We put forward an attack behaviour detection algorithm using triple exponential smoothing and Markov chain. In particular, this algorithm is operated at the base station, which makes the minimum energy consumption of the intermediate nodes. Therefore, they do not need to detect every packet for verifying they are normal or abnormal. And two evaluation factors are considered, the number of the packets and the energy state of the node. These two factors are guaranteed to achieve the accuracy detection. Meanwhile Efficient cluster head selection is necessary for network but set of cluster head suffers from long transmission losses. EE-TLDC has reduced the number of cluster heads which transmit to base station using cluster head hierarchy. EETLDC has improved stability period, make more cluster heads in network. Hierarchy of cluster heads saves energy of network.

XI. FUTURE WORK

A. Try This Scheme with Different Network Protocols

In the future, we want to apply this mechanism to various and different network protocols and improve it for the better energy-efficient based on the existing basis.

B. Secondary Cluster Head Selection

Selection of secondary cluster heads which transmit to base station is done on the basis of their distance from the sink. This work can be extended to optimize the selection of secondary cluster heads. This selection can be done on the basis of residual energy of cluster heads and distance from the base station.

XII. ACKNOWLEDGMENT

We would like to acknowledge the contribution of all the people who have helped in reviewing this paper. Special thanks to my guide prof Mujib Tamboli sir for their immense support while writing this thesis. We would also like to thank our families and friends who supported us in the course of writing this paper.

REFERENCES

[1]. [1] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[2]. [2] C. Krauß, M. Schneider, and C. Eckert, “On handling insider attacks in wireless sensor networks,” Information Security Technical Report, vol. 13, no. 3, pp. 165–172, 2008.

[3]. [3] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” Computer, vol. 35, no. 10, pp. 54–62, 2002.

[4]. [4] J. Deng, R. Han, and S. Mishra, “Defending against path-based DoS attacks in wireless sensor networks,” in Proceedings of the 3rd ACMWorkshop on Security of Ad Hoc and Sensor Networks, pp. 89–96, Alexandria, Va, USA, November 2005.

[5]. [5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: security protocols for sensor networks,” Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.

[6]. [6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hopby- hop authentication scheme for filtering of injected false data in sensor networks,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 259–271, Berkeley, Calif, USA, May 2004.

[7]. [7] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” IEEE Journal on Selected Areas in Communications, vol. 23, no. 4, pp. 839–850,2005.

[8]. [8] C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, “STEF: a secure ticket-based en-route filtering scheme forwireless sensor networks,” in Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES '07), pp. 310–317, Vienna, Austria, April 2007.

[9]. [9] L. Cheng, J. Niu, J. Cao et al., “QoS aware geographic opportunistic routing in wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1864–1875,2013.

[10]. 10] B. Li and L. Batten, “Using mobile agents to detect node compromise in path-based DoS attacks on wireless sensor networks,” in Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing.

[11]. [11] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, “Energy Conservation in wireless sensor networks: a survey”, Ad hoc Networks, Vol. 7, Issue 3, pp.537-568, May 2009.

[12]. [12] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy Efficient communication protocol for wireless microsensor networks”, in the Proc. of the 33rd Annual. Hawaii International Conference on System Sciences (HICSS’00), January 2000.

[13]. [13] S. Lindsey and C.S. Raghavendra, “PEGASIS: Power Efficient Gathering in Sensor Information Systems”, in the Proc of the IEEE Aerospace Conference, Big Sky, Montana, Vol. 3, pp. 1125-1130, March 2002.

[14]. [14] A. Manjeshwar and D.P. Agrawal, “TEEN: a routing protocol for enhanced efficiency in wireless sensor networks”, in 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, Vol. 3, pp. 30189a-30189a, April 2001.

BOOKS

[1] 14.4 Wireless Communication By T.L. Singal, Tata McGraw Hill Publication.

[2] Ilyas M. (2002), The Handbook of Ad Hoc Wireless Networks, CRC Press, Boca Raton, FL, USA.