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
Email: kavitaa.yadav92@gmail.com

Prof Mujib Tamboli
Department of Electronics and Telecommunication Engineering, AIKTC college.
New Panvel, India
Email: mujibtamboli@yahoo.co.in

***Abstract*—** WNS are significantly different from the traditional network architecture due to its wireless communication, energy limitation, and computation constraint and environment of the application. Because of these differences, security becomes a critical issue. The path-based denial of service (PDoS) attacks harm the network maintenance and cause serious damage in the resource constrained WSNs. In a PDoS attack, an adversary 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 creatively propose a novel method, which is operated at the base station to detect the malicious behaviour .The proposed method is combined with triple exponential smoothing and Markov chain, so that it makes the detection results more accurate. Meanwhile, we first use the concept of black hole to defend the PDoS attack in WSNs. Simulation results are provided to evaluate the performance and illustrate the contribution of this mechanism.

***Keywords*—** *Localization; Wireless Sensor Networks (WSNs), Path-Based Denial of service (PDoS).*

*****

I. Introduction

A. An overview on WSN

Wireless sensor network (WSN) is the collection 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 basic 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 features 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. Besides, 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 adversary 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 critical attributes of any communication network. Various attacks have been reported over the last many years. Most of them, however, target wired networks. Wireless networks have only recently been gaining widespread deployment. At the present time, with the advances in technology, wireless networks are 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 accompanied 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 at the same time is its Achilles’ heel. In particular, it makes it extremely easy for an adversary to launch an attack. Denial of Service (DoS). attacks have raised the importance of protecting availability as an aspect of security context, rather than (as previously) only addressing confidentiality and integrity. Attackers use DoS in many different ways, including extortion threats, obfuscation (to hide data exfiltration), hacktivism (to draw attention to a particular cause), and even friendly fire (when a promotion goes a little too well).

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.

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

So there is numerous denial of service attack on network and protocol layer. However there is a different option for its defense. Out of these attack path based denial of service attack is seems 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.

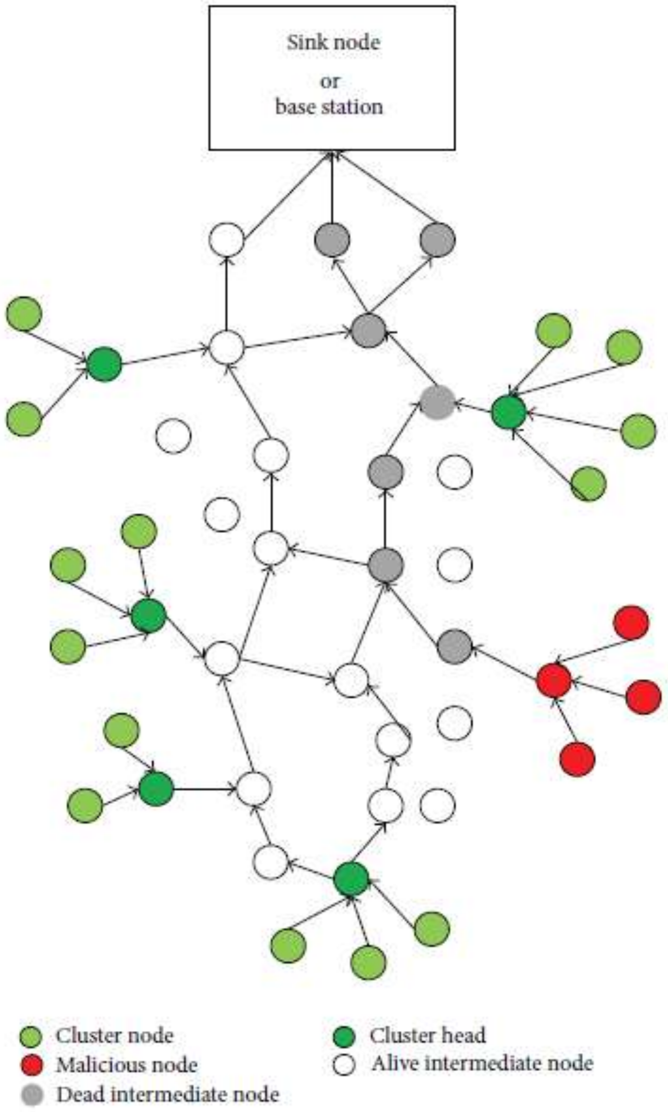

Figure 1: Network attacked by PDoS.

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 copes 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.

The en-route filtering schemes are widely proposed for intermediate nodes filtering the false data, which are generated by malicious aggregator nodes. Besides, they detect intruders engaged in what we have termed PDoS attacks.The basic idea is that the intermediate nodes share some keys with their member nodes in a node group or cluster. Member nodes generate MACs for reporting data by using the shared keys, and intermediate nodes verify the MACs

before forwarding packets [6].

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. Kraub et al. [8] proposed a secure ticket based en-route filtering (STEF) scheme to protect the data report. In the data-report, a certain commitment is added through this scheme and the commitment is created by the hash function such as SHA-256. Therefore, the data-report cannot be modified and forged by an attacker. Their proposed scheme defended against an adversary to inject false data into the sensor network.

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. But this mechanism is designed for the QoS provisioning in WSNs, and, in some respect, it does not meet the requirements of completely defending the DoS attack. Li and Batten [10] proposed a solution that uses mobile agents to detect PDoS attacks easily. But this method is just suitable for the small scale WSNs. Ghosal et al. [11] proposed a dynamic TDMA based scheme, which can defend the PDoS

attacks. However, it is not designed for the PDoS attack; the performance may be dissatisfactory.

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 a novel 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. Meanwhile, inspired by the concept of black hole, we propose the one-hop black holes mechanism to defend the attack packets sent by the compromised CH. In our mechanism, we put the one-hop intermediate nodes away from the attack CH as the black holes, which attract the malicious packets and drop them.Moreover, the one-hop black hole nodes do not receive the normal data packets

IV. SYSTEM ARCHITECTURE

1. ASSUMPTION:

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

2. ADVERSARY MODEL:

The adversary 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. If the adversary is mobile, the resilience scheme can defend the malicious attack.

3. 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.

But in this way there are two challenges that we have to overcome.

- How to effectively and accurately judge that the network is attacked.
- How to validate the PDoS attack as quickly as possible, so that the network can be resolved quickly and reduces the energy consumption. In this section, we adopt triple exponential smoothing of the time series forecasting and the Markov model based on the nodes energy to solve these problems [12, 13].

V. SYSTEM ALGORITHM AND FLOWCHART

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

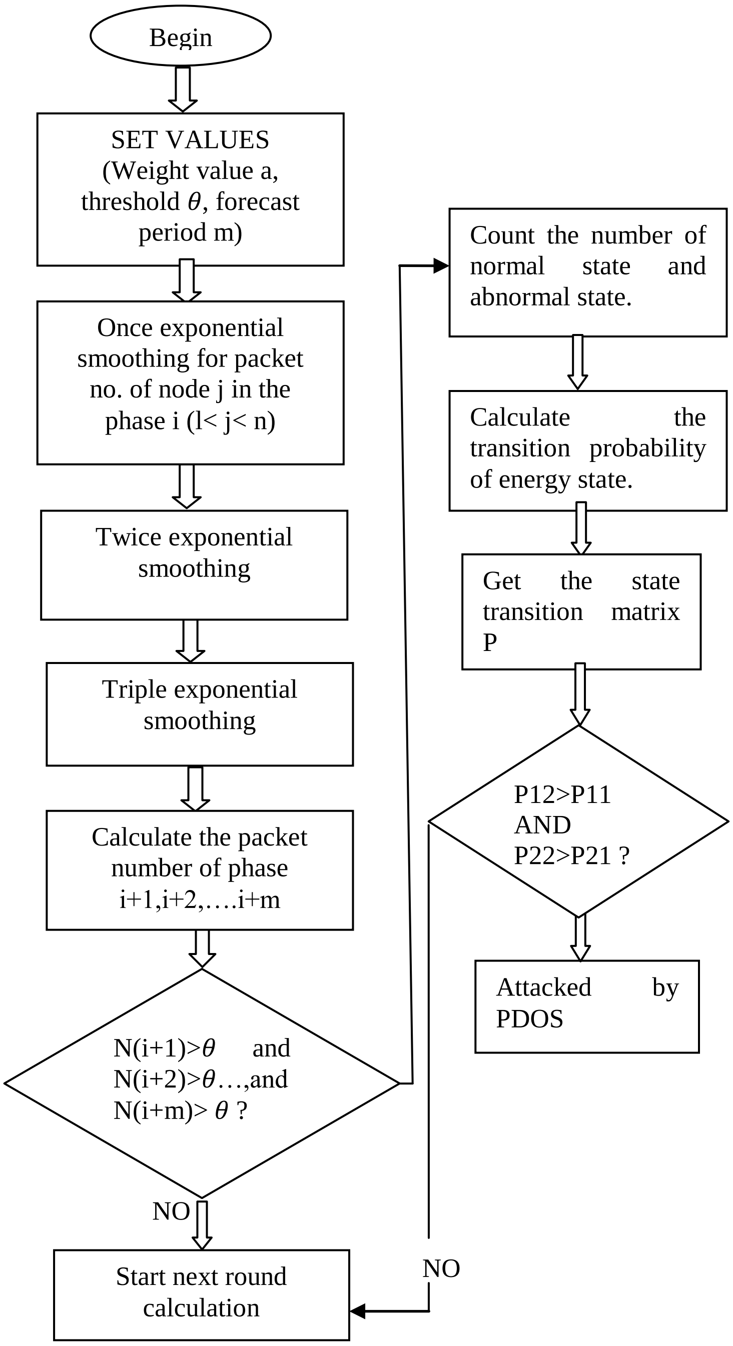
Begin
SET VALUES (Weight value a, threshold θ, forecast period m)
Once exponential smoothing for packet no. of node j in the phase i (l< j< n)
Twice exponential smoothing
Triple exponential smoothing
Calculate the packet number of phase i+1,i+2,….i+m
N(i+1)>θ and N(i+2)>θ…,and N(i+m)> θ ?
NO
Start next round calculation
Count the number of normal state and abnormal state.
Calculate the transition probability of energy state.
Get the state transition matrix P
P12>P11 AND P22>P21 ?
NO
Attacked by PDOS

Figure 3: 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 conformed at the same time.

1. ONE-HOP BLACK HOLES MECHANISM

Just detecting attack behavior is not our ultimate goal because the network is still vulnerable to the PDoS attack. In addition, we are committed to propose an efficient mechanism, which is called one-hop black hole mechanism to defend the PDoS attack and make the attacked network return to normal.

Once the base station or base station detects that the network has been attacked, it also knows the IP address or other information that can uniquely identify the attack node (in this paper, CH is the attack node) through the proposed attack behavior detection algorithm. Then, it is easy to know the location of the adversary and the IP addresses that are one hop away from the adversary node for the base station knows the structure of the network in advance. With this information in hand, the base station will broadcast some specific packets that contain the corresponding IP addresses to the specific intermediate nodes. We call these special packets control packets. And these specific intermediate nodes are the nodes that are one hop away from the compromised CH. The purpose of the control packet is to turn the one hop nodes around the compromised CH into the black holes. In other words, the control packets will transform these one hop intermediate nodes into one-hop black holes. Using the only receiving/not forwarding character of black hole, the one-hop black holes will just receive the attacking packets sent by the compromised CH and then drop them without forwarding. At the same time, they will not receive the normal packets. Then, the attack packets cannot be flooded into the network, and the network successfully defends the PDoS attack. Figure 4 shows how the one-hop black holes defend the PDoS attack.

2. AODV Protocol

AODV is an on demand routing protocol and is capable of both unicast and multicast routing. It establishes routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the source nodes. Additionally, the AODV protocol forms tree structure which connects multicast group members. The trees are composed of the group members, and the nodes need to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and large scales of member nodes.

There are three main message types in the AODV protocol, which are route requests (RREQs), route replies (RREPs), and route errors (RERRs). Herein, we mainly introduced the RRER packets, because the following control packet is designed and modified by the RRER packets.

3. Modification of the SMAC Protocol

However, there is an important challenge that we should solve. If the network has been attacked in a period of time, which means the attacking path has been established. The control packet cannot be received by the black hole nodes since they are busy with forwarding the attacking packet. In order to handle this problem, we make a little modification on the SMAC protocol. SMAC mechanism allows nodes to sleep periodically after a certain time of listening for reducing energy consumption.

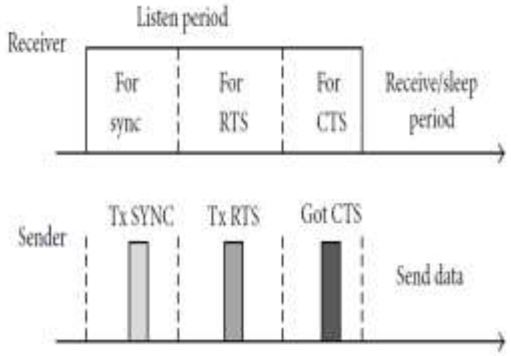

Figure 5: The frame structure of the SMAC

Figure 5 describes the frame structure of the SMAC protocol. If the attacking path has been established, the SMAC needs to continue the receiving state and receives the attacking packets. Here, we add a timer in the SMAC, setting a threshold T for receiving state.

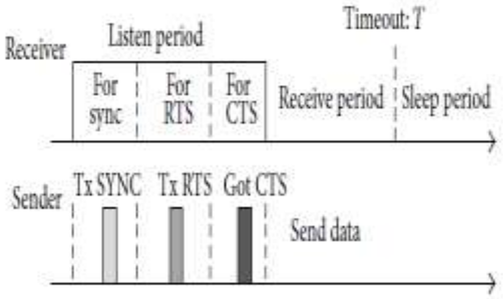

FIGURE 6: The revised structure of the SMAC.

As illustrated in Figure 6,the receiving state will be forced into sleep state if timeout. The value of T can be set initially and adjusted through the practical application. It would be specially mentioned that there is no a unique optimized value of T. According to the observation of our simulation, while the sending rate of the attack packet is different, the defend the attack with the shortest time. Then, the control packet may defeat the attacking packets when they compete with each other for the media at the new frame. Besides, the control packet can be successfully received by the one-hop nodes of the compromised. As the mentioned before, these nodes are able to become the black holes and defend the PDoS attack.

VII. SIMULATION

The simulation is conducted on ns2 simulator,and used parameters are shown in table 1.

SIMULATION PARAMETER	**VALUE**
Node number	50
Base station number	1
Compromised CH number	1
Initial power	20(j)
Packet size	1000(bit)
Normal packet average rate	0.1(Mb/s)
Abnormal packet average rate	0.5(Mb/s)
Threshold θ	15000(packets)
m	2

Table 1.Simulation parameters

We experiment a scenario to simulate the energy consumption of intermediate nodes.

VIII. CONCLUSION

In this paper, we propose a novel solution to defend the PDoS attack. We put forward an attack behavior 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, into completely defend the PDoS attack. we propose one hop black holes mechanism, which makes the intermediate nodes that are one hop away around the malicious CH as the black holes. These nodes can just receive the attacked packets which are sent by malicious nodes and drop them. In addition, we design the recovery scheme for the one-hop black hole nodes to make the whole mechanism more flexible. In the future, I experiment the scenario to stimulate the energy consumption of intermediate nodes. Find the expected result using NS2 simulator.

Acknowledgment

We would like to acknowledge the contribution of all the people who have helped in reviewing this paper. We would also like to thank our families and friends who supported us in the course of writing this paper.

References

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

[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] 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] 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 onSecurity and Privacy, pp. 259–271, Berkeley, Calif, USA, May 2004.

[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] 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] 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] 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 onWireless Communications, Networking and Mobile Computing.

[11] Dr.Suryaprasad J, Praveen Kumar B O, Roopa D Arjun A K, A Novel Low-Cost Intelligent Shopping Cart, Proceedings of the 2nd IEE International Conference on Networked Embedded Systems for Enterprise Applications NESEA 2011, Perth, Australia, December 8-9, 2011.

[12] Swati Zope, Prof. .MarutiLimkar, “RFID based Bill Generation and Payment through Mobile”,International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 3, June 2012.

[13] G. Roussos and B. College, “Enabling RFID in Retail”, Computer, IEEE, vol. 39, no. 3, 2006, pp. 25-30.

[14] Saurabh Kumar Sultaina, GouravJaiswal, PrateekJain “RFID Based Automatic Shopping Cart ” CONTROL THERORY& INFORMATICS ISSN 2224- 5774(PRINT) ISSN2225-0492(ONLINE), VOL1, NO1, 2011.

[15] Vanitha “Smart Shopping Experience Based On RFID”International Conference on Computing and Control Engineering (ICCCE2012), 12&13 APRIL, 2012

[16] Sachita Roy, UditaGangwal, JyotsanaBapat, Robert Bakker, Edwin Keijsers, and Hans van der Beak “Smart Shopping Cart For Automated Billing Purpose Using Wireless Sensor Networks” the seventh international conference on sensor technologies &applications.

[17] S. Sainath, K. Surender, V. Vikram Arvind, J. Thangakumar“Automated Shopping Trolley for Super Market Billing System” International Journal of Computer Applications (0975 – 8887).

[8] Kalyani Dawkhar1, Shraddha Dhomase2,Samruddhi Mahabaleshwarkar “Electronic Shopping Cart For Effective Shopping based on RFID” international journal of innovative research in electrical, electronics, instrumentation and control engineering Vol. 3, Issue 1, January 2015.

[9] Savi Technologies. ”Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility, SAVI Technology.”