International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 2, pp: (355-361), Month: April - June 2015, Available at: www.researchpublish.com

Prevention of Carousel Attacks in Wireless Sensor Network

[1]Mr.K.Kannadasan, [2]K.Sivananthini

[1]Assistant Professor, Dept. Of ECE, Adhiparasakthi Engineering College, Melmaruvathur, TN, India
[2]Final Year M.E (Applied Electronics), Dept. Of ECE, Adhiparasakthi Engineering College, Melmaruvathur, TN, India

Abstract: **The WSN (wireless sensor network), has attracted researchers attention due to its wide range of potential applications. The sensor nodes may become faulty due to low battery power or some other physical defects. The faulty nodes may badly effect the network performance. In carousel attack, an adversary sends a packet with a route composed as series of loops, such that the same node appears in the route many times. The attack increases the power consumption of the network and depleting the lifetime of battery. It is providing the security by implementing cellular automata. Due to the prevention of carousel attack, the power consumption is reduced.**

Keywords: **Carousel Attack, Wireless sensor network, security, simulation, Cellular Automata.**

1. INTRODUCTION

The wireless sensor network are used to sense and monitor a wide range of ambient conditions. In such a network, hundreds of sensor nodes are deployed randomly with the ability to capture events, perform some computations, and to communicate with the neighbors. The sensors are deployed in remote or hostile environment, where recharging of battery is quite impossible. That is, the sensors have to work for a long period of time without recharging. Therefore, the battery power consumption is major concern in a WSN. Wireless networks of sensors are likely to be widely deployed in the near future. Because greatly extend the ability to monitor and control the physical environment from remote locations and improve accuracy of information. It obtained via collaboration among sensor nodes and online information processing at those nodes.

Security measures to prevent vampire attacks are orthogonal to those used to protect routing infrastructure and do not protect against vampire attacks. The intruder may attack any node in a network. It carefully monitors all the nodes in a network and attacks a nearest node. The victim node can be a normal node or a cluster head. Vampire attacks are not protocol specific, in that they do not rely on design properties. Vampire attacks as the composition and transmission of a message that causes more energy to be consumed by the network than an honest node. The usage of energy by malicious nodes is not considered, since they can always drain the life time of battery. Vampire are more resource constrained than honest nodes. Vampire attack deplete the battery power of the network. The proposed method in this paper is novel in the sense that we aim at cellular automata.

1.1 Classification:

Denial of service is an attack, where a victim can use 10 minutes of the CPU time to transmit a data packet, but whereas an honest node uses 1 minutes of its CPU time to transmit the same data packet. In multihop routing network a source compose the shortest path and transmits the data packet to the next hop, which transmits it further, until the destination is reached; consuming the resources not only at the source node but also at every node the packet moves through. Vampire attack can be defined as a voluntary action of composing and transmitting a malicious messages that chooses the longest path which consumes more energy of the network than if an honest node transmits a message of identical size to the same destination. The strength of an can be measured by the ratio of network energy used in the honest case to the energy used in the malicious case

1.2 Protocols:

Here we consider a stateful routing protocol, AODV (Ad-hoc On Demand Distance Vector). In stateful protocol, the network nodes are aware of the network topology and its state, and make local forwarding decisions based on that stored state. Two important classes of stateful protocols are link-state and distance-vector. In link-state protocols, such as GPSR, nodes keep a record of the up or down state of links in the network, and flood routing updates every time a link goes down or a new link is enabled. Distance –vector protocols like DSDV keep track of the next hop to every destination, indexed by a route cost metric, e.g., the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated.

1.3 Vampire Attacks:

Vampire attacks are very difficult to detect and prevent. These attacks deplete the node's battery power of the network. There are two types of vampire attack:

1. Carousel Attack
2. Stretch Attack

By doing so we are evaluating the vulnerability of existing protocols.

The adversary composes packets with purposely introduced routing loops. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. This strategy can be used to increase the route length. Carousal attacks are the one in which the adversary packet will create a route to the destination that consists of a number of loops thereby increasing the energy consumption by the networks.

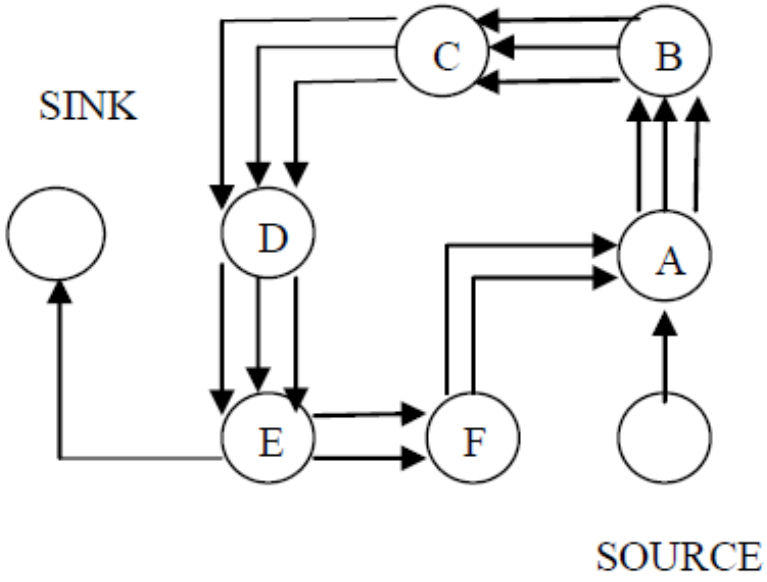

Fig.1. Carousal attack

Figure 1 shows carousal attack in which the source sends a packet to the sink. The figure shows the network under attack where the packets are sent in loops causing more usage of energy and time. The packet from the source will reach to the destination only after the traversal of packet more than once through the same nodes. Here the length of the route will be greater than the number of nodes of the network. It is affected by the position of the adversary's position of the adversary in relation to the destination. So the adversary's position is important to the success of this attack. Hence the maximum power will be drained from each node that is participating in the routing of packets.

Stretch attack targeting a source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. It increases the packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. Stretch attacks constitute the process of making the packet to be traversed through almost every node in the networks.

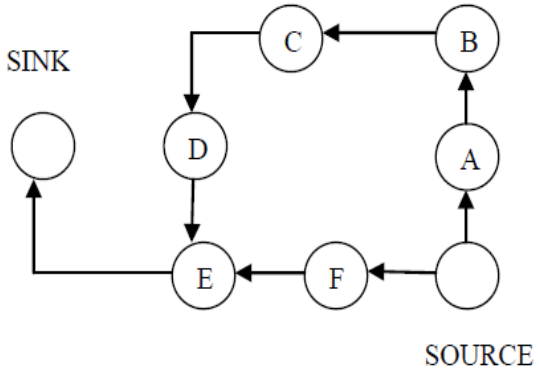

Fig.2. Strech attack

It is called stretch attack since it lengthens the packet path causing the packet to be traversed through a number of nodes in the network. Hence it diverts the packet to be transferred from the optimal path. Figure 2 shows an example of stretch attack in which the packet is diverted from the optimal path. Here instead of traversing the packet from the node source to sink, it makes the route to the nodes to take part in the routing process. Hence the powers of these nodes get wasted. In this way stretch attack causes the drainage of the power from the nodes that are not necessary to take part in the routing.

This paper focuses mainly on the carousel attack. Carousel attack can be reduced by making the intermediate node to replace the part or the entire route if they know a better path to the destination.

1.4 Mitigation Of Attacks:

The carousel attack can be prevented entirely by having forwarding nodes and check source route for loops. While this adds extra forwarding logic and thus more overhead, we can expect the gain is to be better in malicious environments. When a loop is detected, the source route could be corrected and the packet sent on the network. But one of the attractive features of source routing is that the route can itself be signed by the source. The AODV protocol does implement loop detection, but confusingly does not use it to check routes in forwarded packets. Therefore, it is better to simply drop the packet, especially considering the sending node is likely malicious.

The stretch attack is more challenging to prevent. The forwarding node not checking for optimality of the network is the success of the stretch attack. We can bound the damage of carousel and stretch attackers by limiting the allowed source route length based on the expected maximum path length in the network. But we would need a way to determine the network diameter.

2. CELLULAR AUTOMATA

A Cellular Automata (CA) is a collection of cells arranged in a grid, such that each cell changes state as a function of time according to defined set of rules that includes the state of neighboring cells. The simplest class of one dimensional cellular automata, elementary cellular automata have two possible values for each cell (0 or 1), and rules that depend only on nearest neighbor values. This work proposes a scheme CA, developed around the cellular automata for efficient management of battery power in sensor nodes with optimized cost of implementation. Each sensor node is assumed to be equipped with a segment of the cellular automata. It selected for the network that defines the state active/standby of the node at next time instant. The CA based management of status active/standby of a node ensures the reduced battery power consumption in nodes of a cluster as well as in the whole sensor network.

The simulation results establish that the CA can better utilize resources and ensure a maximally covered energy efficient sensor network. The CA based scheme that can be efficiently identify the faulty nodes of a WSN operation. The scheme is developed around the Single Attractor Cellular Automata (SACA).

2.1. One Dimensional Cellular Automata:

A one-dimensional cellular automaton consists of two things. A row of cells and a set of rules. Each of the cells can be in one of several states. The number of possible states depends on the automaton. A CA doesn't just sit there. Over time, the cells can change from state to state. The cellular automaton's rules determine how the states change. It works like this when the time comes for the cells to change state, each cell looks around and gathers information on its neighbors' states.

Exactly which cells are considered neighbors is also something that depends on the particular CA Based on its own state, its neighbors' states, and the rules of the CA, the cell decides what its new state should be. All the cells change state at the same time.

2.2. Two Dimensional Cellular Automata:

Cellular automata are mathematical models for systems in which many simple components act together to produce complicated patterns of behavior. One-dimensional cellular automata have now been investigated in several ways. Its presents an exploratory study of two-dimensional cellular automata. The extension to two dimensions is significant for comparisons with many experimental results on pattern formation in physical systems. Immediate applications include crystal growth, reaction-diffusion systems, and turbulent flow patterns. The effectiveness of CA based diagnosis scheme in VLSI circuits encourages the design of a CA based scheme for faulty node diagnosis in WSN.

2.3. Reversible Cellular Automata:

The reversible cellular automata likewise the carousel attack. A reversible cellular automata is a cellular automata in which every configuration has a unique predecessor. The source node send a packet to the next node and the process will be continued, the packets are return to the same source node. It does not reach the destination node. That is, it is a regular grid of cells, each containing a state drawn from a finite set of states.

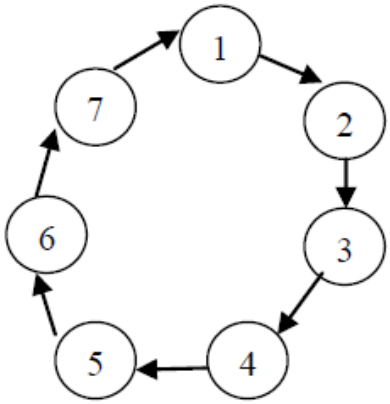

Fig.3. Reversible cellular automata

Figure 3 shows the A CA is reversible if states form only cycles in the state transition diagram. Node 1 send the packet to node 2, then continuously the packets are send to next node and finally the packets are reach the same node. Reversible computing is a paradigm where computing models. This effectively leads to deviation from the desired outcome, ineffective utilization of network bandwidth and unproductive computational overhead. Reversible cellular automata form a natural model of reversible computing, a technology that could lead to ultra-low-power computing devices. Properties related to reversibility may also be used to study that CA are not reversible on their entire configuration space.

2.4. Irreversible Cellular Automata:

A CA is irreversible if states does not form a cycles in the state transition diagram.

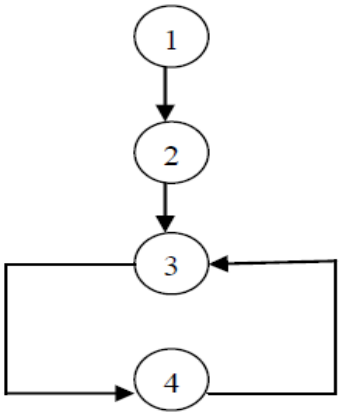

Fig 4 shows the irreversible cellular automata. In irreversible cellular automata the packets are does not reach the source node and the packets are send to destination node through the intermediate nodes. Computation can often be carried out in a very different manner from conventional computing systems. The irreversible cellular automata provide a model of parallel computation that mimics the dynamics of the actual physical world more closely than non reversible model. Their reversibility corresponds to the microscopic reversibility of physical system. To compare both the reversible and irreversible cellular automata, we are using the irreversible cellular automata by prevent the carousel attack.

3. SIMULATION RESULTS AND DISCUSSION

The execution were carried out in PC with network simulator (ns-2). It is one of the most popular simulator among networking researchers. It is discrete event packet level simulator, events like "received an ACK packet" enqueued a data packet. Network protocol stack written in c++. TCL used for specifying scenarios and events. It simulates both wired and wireless networks. Pre-processing are used to generate the traffic and topology generators. Post processing used to simple trace analysis often in awk, perl, or tcl.

The topology consist of two mobile nodes and the nodes are move about within 500m×500m area. A tcp connection is setup between the two mobile nodes. Packets are exchanged between the nodes as come within hearing range of one another. As move away packet start getting dropped. The god stores the number of mobile nodes table of shortest number of hops required to reach from one node to another. The performance of WSN is analyzed by employing CA. CA has been implemented in the wireless sensor network to mitigate the Carousel attack.

Plot for energy consumption with increasing number of hops to destination is clearly shown in Figure 3.1. The x axis denotes the number of hops and y axis denotes the energy consumption. The energy consumption of the network with carousel attack and after mitigation of carousel attack is plotted. After mitigation of carousel attack the energy consumption is decreased considerably.

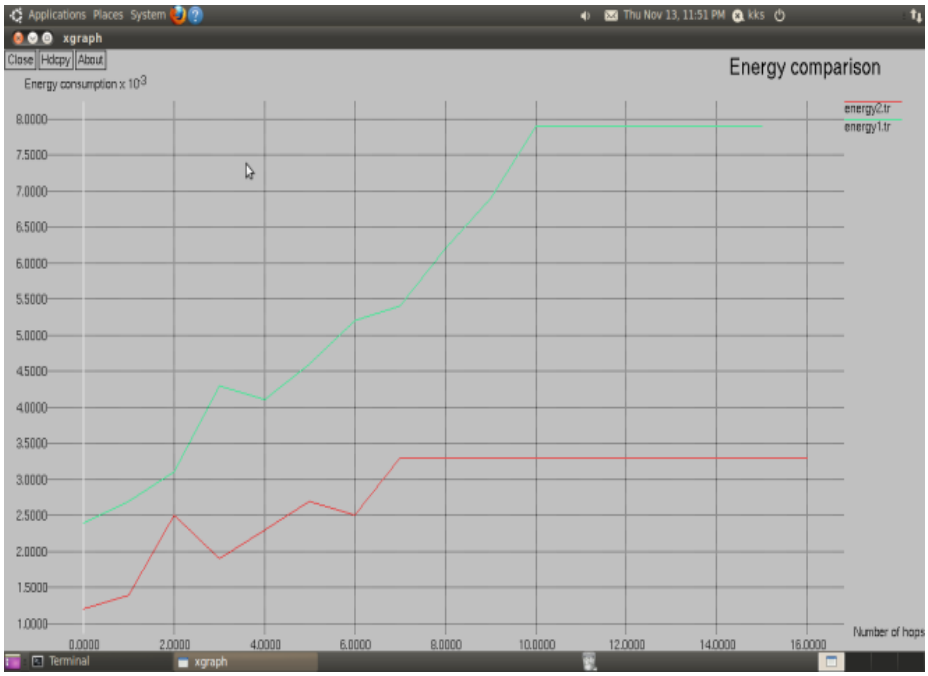

Figure 3.1 Comparison of energy consumption of network with Carousel attack and mitigation of Carousel Attack

Plot for number of hop versus delay is computed and simulated for varying number of hops. This graph was compared to the energy consumption of carousel attack and after prevention of carousel attack. The power consumption is decreased compared to the carousel attack. Power consumption is increased in carousel attack. So reduce the power consumption using the CA. From this simulation result it is clear that the delay increases when number of loop formation increases. Fig 3.2 shows the calculation of delay for WSN. The x axis denotes the number of hops and y axis denotes delay. Carousel attack always forms the loop, so the delay also increases. After mitigation the loop count decreases and the time taken by the packet to reach the destination is reduced, thereby reducing the delay.

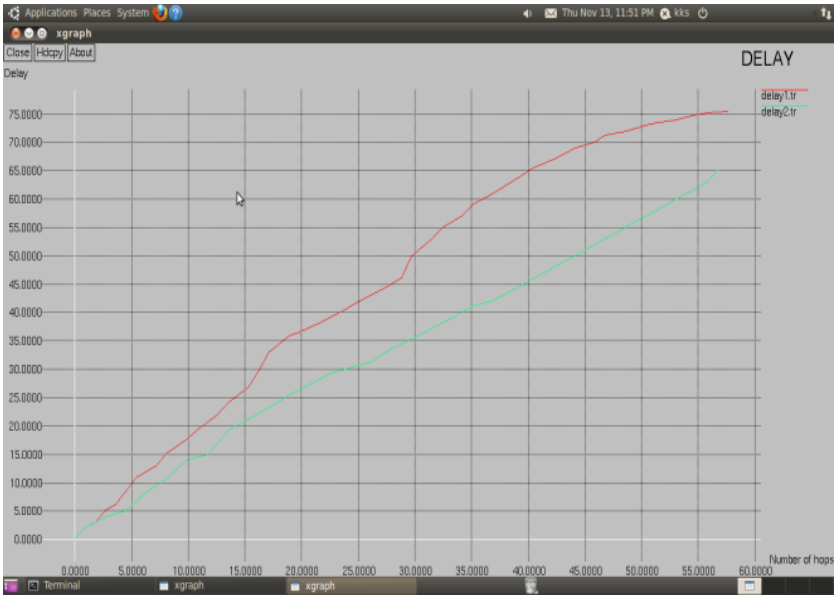

Figure 3.2 Calculation of delay for Wireless Sensor Network

Plot for throughput shows that, if the energy consumption of the network decreases, throughput of the network also increases. In Figure 3.3 shows the x-axis indicates efficiency and y-axis indicates throughput. This graph was compared to the throughput of carousel attack and after prevention of carousel attack. The throughput is decreased compared to the carousel attack. Throughput is increased in carousel attack. So reduce the throughput using the CA. Throughput is the rate of production or the rate at which something can be processed. The throughput of a communication system may be affected by various factors, including the limitations of underlying analog physical medium, available processing power of the system components, and end-user behavior

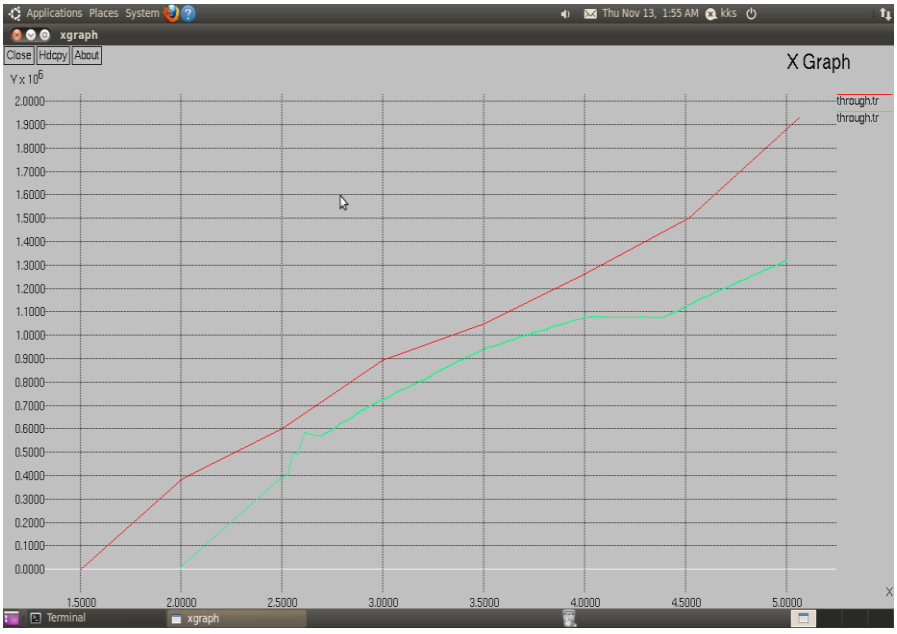

Figure 3.3 Comparison of throughput of network with Carousel attack and mitigation of Carousel attack

4. DISCUSSIONS

It focuses on implementing the Cellular Automata in mitigates the Carousel attack on wireless sensor network. Implementation of Cellular Automata improves the performance of WSN by reducing the number of loops. Because of absence of loop power consumption of the network is considerably reduced. As power consumption decreases efficiency is increased considerably.

5. CONCLUSION

The reduction in the power consumption of node using cellular automata had been worked out. Using cellular automata in vampire attack network provides the maximum security by using not as much of power consumption. To achieve the better security by using cellular automata compared to no back tracking method. The energy consumption in the case of cellular automata implemented in the network is same as that of honest node. Similarly reduction in the power consumption increases the battery life time.

REFERENCES

[1] Eugene Y.Vasserman and Nicholas Hopper, "Vampire Attacks:Draining Life from Wireless Ad Hoc Sensor Networks," IEEE Transaction On Mobile Computing,vol.12,no.2,February 2013.

[2] Aad. I, Hubaux. J. P, and Knightly. E.W, (2004), "Denial of Service Resilience in Ad Hoc Networks," Proceedings of Association for Computing Machinery Mobile Communication, vol. 3, no. 5.

[3] Acs. G, Buttyan. L, and Vajda. I, (2006), "Provably Secure On- Demand Source Routing in Mobile Ad Hoc Networks," IEEE Transaction on Mobile Computing, vol. 5, no. 11, pp. 1533-1546.

[4] Bellardo. J, and Savage. S, (2003), "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proceedings of 12th Conference United States ENIX Security, vol. 4, no. 2.

[5] Chang. J. H, and Tassiulas. L, (2004), " Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/Association for Computing Machinery Transaction on Networking, vol. 12, no. 4, pp. 609-619.

[6] Deshmukh. R, and Potgantwar. D, (2014), " Prevention of Vampire Attacks in Wireless Sensor Network Using Routing Loop," Proceedings of International Religious Federation International Conferences, vol. 4, no. 12.

[7] Feeney. L. M, (2001), " An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks,"Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249.

[8] Goldsmith. A. J, and Wicker. S. B, (2002), " Design Challenges for Energy Constrained Ad Hoc Wireless Networks," IEEE Wireless Communication, vol. 9, no. 4, pp. 8-27.

[9] Hill. J. L, and Culler. D. E, (2002) ," Mica: A Wireless Platform for Deeply Embedded Networks," IEEE Micro Magazine on science, vol. 22, no. 6, pp. 12-24.

[10] Ilora Maity, Gunjan Bhattacharya,Sukanta Das, and Biplo sikdar, (2011) , " A Cellular Automata Based Scheme for Diagonosis of Faulty Nodes in WSN," IEEE Conference on System, vol.7495, pp. 234-243.

[11] Indrajit Banarjee, Sukanta Das, Hafijur Rahaman, and Biplab Sikdar, (2006), "An Energy Efficient Monitoring of Ad-Hoc Sensor Network With Cellular Automata," IEEE International Conference on Systems, Man, Cybernetics, Vol. 2, no. 7.

[12] Jacquet. P, Muhlethalu. P, Clausen. T, and Laouiti. A, (2003), "Optimized Link State Routing Protocol for Ad-Hoc Networks," Hypercom Project, Vol. 2, no. 2.

[13] Raymond. D. R, Marchany. R. C, Brownfield. M. I, and Midkiff. S. F, (2009), "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Transaction on Vehicular Technology, vol. 58, no. 1, pp. 367-380.

[14] Sandeep Kumar, (2001), "An Intelligent Defence Mechanism for Security in Wireless Sensor Network," IEEE Conference on protocol, vol. 4, no. 3.

[15] Shantala Patil, Vijaya Kumar. B. P, Sonali Singha, and Rashique Jamil, (2012), " A Survey on Authentication Techniques for Wireless Sensor Network," Interscience and technology, vol. 7, no.11.