ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

Security to Data Transmission over Wireless Sensor Network

Vicky G. Saokar [1], Y B Jadhao[2]

P.G. Student, Department of Computer Engineering, Dr.VBKCOE, Malkapur, MH, India[1]

Assistant Professor, Department of CSE, Dr.VBKCOE, Malkapur, MH, India[2]

ABSTRACT: The management of ADHOC network is great challenge due to dynamic infrastructure and mobility of node. Due to mobility of node routing path of network and security of communication suffered. In the process of node mobility and path discovery of routing protocol take huge amount of power and decrease the life of network. For the improvement of power and secured communication various protocol are designed but all are limitation in terms of group communication in ADHOC network. In this dissertation we modified the secured stateless protocol for secured routing and minimized the utilization of power during path discovering and establishment. For the authentication of group node used group signature technique and sleep mode threshold concept for power minimization.

Our proposed modified scheme "secured backup routing protocol with minimization of power consumption" simulate in NS-2 simulator. In simulation process we used 25 normal nodes and 2 abnormal nodes. The evaluation of perform ace is measured by packet delivery ratio, normalized load, packet throughputs and also evaluate the life time of network or sleep mode energy of node. Our modified scheme is compared with existing SBPAODV and good results in compare with old method. These process previously used in MOAODV protocol, but in this dissertations we used AODV protocol for routing protocol.

KEYWORDS: ADHOC Network, WSN.

I. INTRODUCTION

Wireless sensor networks are a new type of networked systems. Wireless nodes and is used in a variety of applications such as military sensing and tracking, environmental monitoring, disaster management, etc. Due to the nature of the military, it is obvious that the data is of a private nature and is required to remain this way to ensure the success of the application. Enemy tracking and targeting are among the most useful applications of wireless sensor networks in military terms. Characterized by severely constrained computational and energy resources. [1] When the wireless sensor networks are implemented in open, un-monitored hostile terrain, security becomes extremely important because different of malicious attacks. It is main issue security in wireless sensor networks has attracted a lot of attention in the recent year Nowadays, there is a growing interest in Wireless Sensor Networks WSNs are multiple mesh networks made of lots of small battery powered sensors that generate data about the environment in the Moreover, they set wireless communication capabilities allowing them to exchange data. The low capabilities of the sensors, their wireless communications, and the fact that they are deployed in open areas make them attract to attacks. Routing is a important issue in WSNs. Here, we consider a routing scheme called converge cast routing. In this problem, a node is distinguished as the sink and all non-sink nodes, called source nodes, must be able to transmit data to the sink on request. The sink can be arbitrary [3] far from other nodes. Importantly, in WSNs, source nodes are sensors and the sink is a base station that is linked to another network, like a gateway.

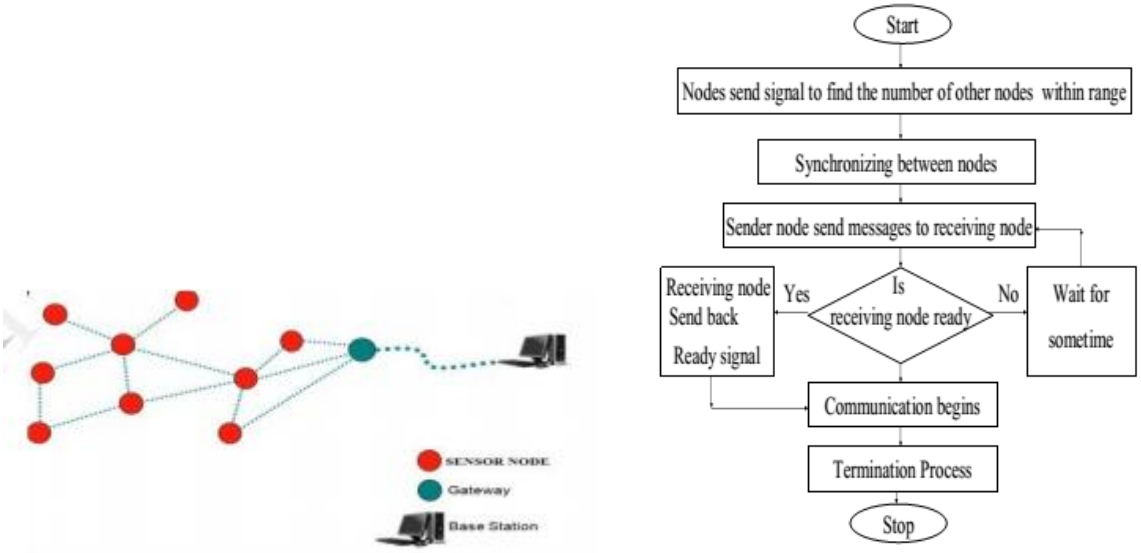
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018



(a) (b)

Figure 1: (a) Architecture of WSN (b) Working of general AdHoc Network

II. PROBLEM DEFINITION

In the WSN most important part is security. A wireless sensor network is composed of tiny sensor nodes each capable of sensing some phenomenon, doing some limited data processing and communicating with each other [7]. These tiny sensor nodes are deployed in the target field in large numbers and they collaborate to form an adhoc network capable of reporting the phenomenon to a data collection point called sink or base station. These networked sensors have man potential civil and military applications i.e., intrusion detection, habitat and other environmental monitoring related applications etc.

Coverage Holes

Although the coverage problem has been interpreted in a variety of ways in the existing literature, we follow [9] for defining the coverage hole problem as follows. Given a set of sensors and a target area, no coverage hole exists in the target area, if every point in that target area is covered by at least k sensors, where k is the required degree of coverage for a particular application.

Routing Holes

A routing hole consists of a region in the sensor network where either node are not available or the available nodes cannot participate in the actual routing of the data due to various possible reasons. These holes can be formed either due to voids in sensor deployment or because of failure of sensor nodes due to various reasons such as malfunctioning, battery depletion or an external event such as _re or structure collapse physically destroying the nodes.

Jamming Holes

An interesting scenario can occur in tracking applications when the object to be tracked is equipped with jammers capable of jamming the radio frequency being used for communication among the sensor nodes [10]. When this happens, nodes will still be able to detect the presence of the object in the area but unable to communicate the occurrence back to the sink because of the communication jamming.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

III. PROPOSED DESCRIPTION SOFTWARE

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done usingNS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors .Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field .Among these are the University of California and Cornell University who developed the REAL network simulator,[1 2] the foundation which NS is based on. Since 1995 the Defence Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual Inter Network Test bed (VINT) project [9].2 currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile. Main NS2 Simulation Steps The followings show the three key step guideline in defining a simulation scenario in a NS2

Step 1: Simulation Design The first step in simulating a network is to design the simulation. In this step, the users should determine the simulation purposes, network configuration and assumptions, the performance measures, and the type of expected results.

Step 2: Configuring and Running Simulation This step implements the design in the first step. It consists of two phases: Network configuration phase: In this phase network components (e.g. node, TCP and UDP) are created and configured according to the simulation design. Also, the events such as data transfer are scheduled to start at a certain time. 2.6 A Simulation Example 27 Simulation Phase: This phase starts the simulation which was configured in the Network Configuration Phase. It maintains the simulation clock and executes events chronologically. This phase usually runs until the simulation clock reached a threshold value specified in the Network Configuration Phase In most cases, it is convenient to define a simulation scenario in a Tclscripting file (e.g., <file>) and feed the file as an input argument of an NS2 Invocation (e.g., executing "ns <file>").

Step 3: Post Simulation Processing the main tasks in this step include verifying the integrity of the program and evaluating the performance of the simulated network. While the first task is referred to as debugging, the second one is achieved by properly collecting and compiling simulation results.

IV. EXPERIMENTAL RESULTS

TABLE-I SIMULATION PARAMETER

Parameter	value
Simulation duration	100 sec
Simulation area	1000*1000
Number of mobile node	25
Traffic type	Cbr(udp)
Packet rate	4 packet/sec
Abnormal node	2
Host pause time	10sec

We simulate our method in NS-2 with help of OTCL & TCL simulation script file, now evaluation of performance of these modified scheme we used standard parameter of adhoc network.

Throughput: It gives the fraction of the channel capacity used for useful transmission (Data packets correctly delivered to the destination) and is defined as the total number of packets received by the destination. It is in fact a measure of the effectiveness of a routing protocol.

Average end-to-end delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

Packet delivery fraction: The ratio of the data packets delivered to the destinations to those generated by the traffic sources.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

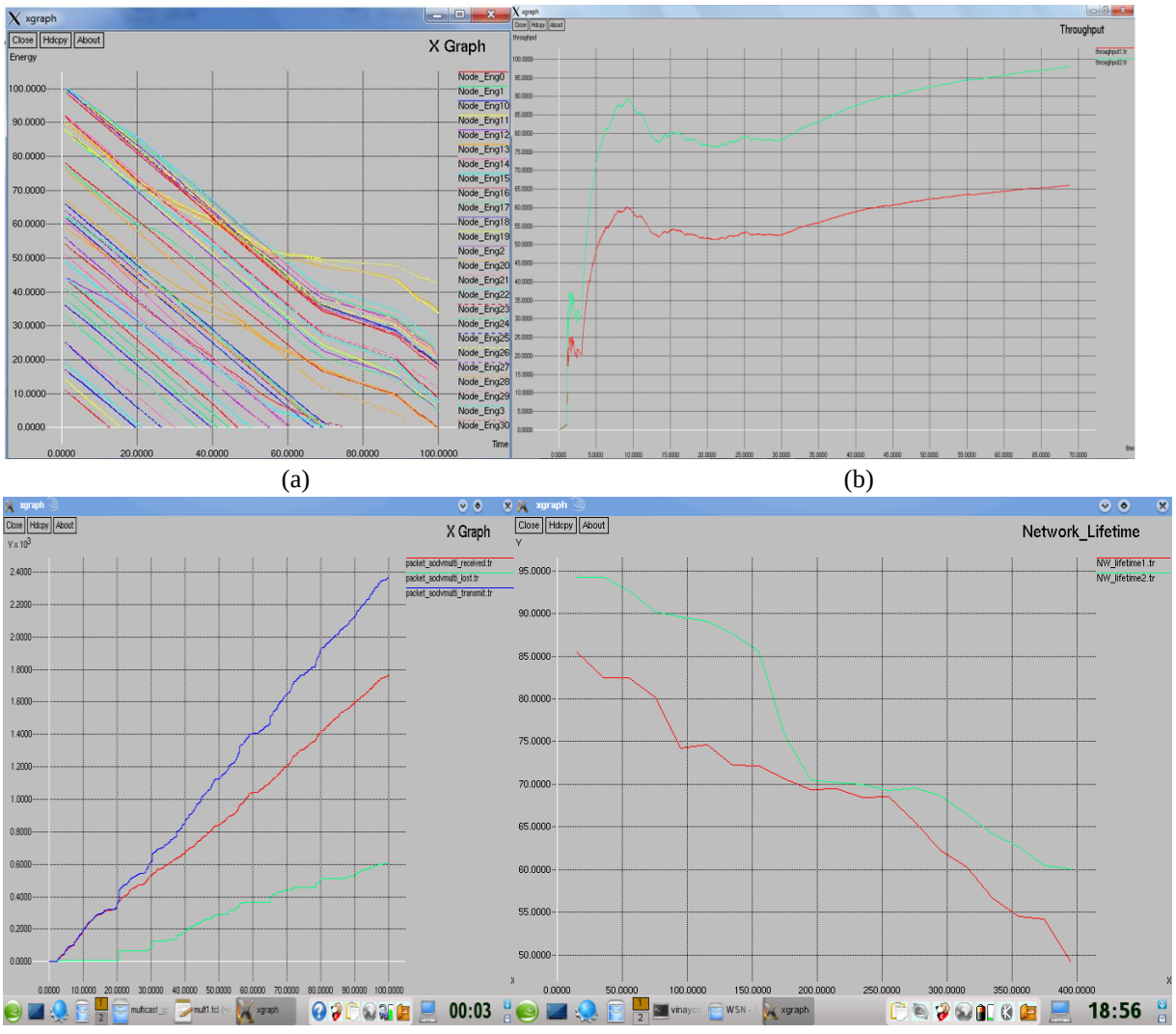


Fig. 2 (a) shows the power consumption of mobile node in given scenario of mobile node. (b) Shows that throughput of packet send and received during attacking mode. (c) Shows that packet transmits and received packet ratio during attacking mode during communication of group node. (d) Shows that network life time of simulated node in given scenario.

V. CONCLUSION

In this dissertation we modified the SBPAODV routing protocol for secured communication and energy efficient process. Our proposed model reduces the consumption of energy value during control messaging. The reduced power of consumption increases the life time of network. For the authentication of group node used group signature technique and sleep mode threshold concept for power minimization. The proposed algorithm divide node in two states sleeps mode and active mode. The processes of going node sleep to active mode calculate priority of all sleep nodes and compare with arithmetic mean of threshold. The value of sleep mode greater and equal to threshold thus acts as master node in group. In this fashion the utilization of power minimized on time of group communication. Our experimental result shows maximum life time network in comparison to SBRP routing protocol. In future we also

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

improved the key authentication mechanism in group communication. Our proposed mechanism has overcome some of the limitations like it has the miss some group node request during group communication. It also introduces little bit computational overhead during route advertisement and path establishment.

REFERENCES

[1] Mustafa Bani Khalaf, Ahmed Y.Al-Dubai and William Buchanan "A New Adaptive Broadcasting Approach for Mobile Ad hoc Networks",978-1-4244-7071-6/10/$26.00 ©2010 IEEE
[2] Mr. Sandeep Gupta Prof.Abhishek Mathur "Enhanced Flooding Scheme for AODV Routing Protocol in Mobile Ad hoc Networks" ,2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies
[3] Mozmin Ahmed, Md. Anwar Hussain, "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks"
[4] Zhimu Huang, Ryo Yamamoto, Yoshiaki Tanaka, "A Multipath Energy-Efficient Probability Routing Protocol in Ad Hoc Networks" Feb 16-19 ICATE2014
[5] Akshay Aggarwal, Savita Gandhi, Nirbhay Chaubey, Keyurbhai A Jani "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 Fourth International Conference on Advanced Computing & Communication Technologies
[6] Jih-ching Chiu1, Chun-Yao Zheng, Yao-Chin Huang and Kai-Ming Yang, "Design and Implementation of Sequential Repair and Backup Routing Protocol for Wireless Mesh Network"
[7] D. Sandhiya K. Sangeetha R.S. Latha, "Adaptive Acknowledgement Technique with Key Exchange Mechanism for MANET"
[8] Neha Shirke, Kishor Patil, Shriram Kulkarni, Shriram Markande, "Energy Efficient Cluster based Routing Protocol for Distributed Cognitive radio network" 978-1-4799-3486-7/14/$31.00_c 2014 IEEE.
[9] Aarfa Khan Prof. Shweta Shrivastava, Prof. Vineet Richariya, "Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA)" 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.
[10] Jyoti Joshi, Vidhate Amarsinh, "Enhanced 2ACK Scheme to Prevent Routing "Misbehavior Using OLSR Protocol." 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.
[11] Mallapur Veerayya, Vishal Sharma and Abhay Karandikar "Sq-Aodv: A Novel Energy-Aware Stability-Based Routing Protocol for Enhanced Qos In Wireless Ad-Hoc Networks" IEEE 2012.
[12] Seema Verma Pinki Nayak and Rekha Agarwal" Energy Efficient Routing in Mobile Adhoc Networks based on AODV Protocol " in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 2, November 2012
[13] S. Narayanaswamy, V. Kawadia, R. Sreenivas, and P. Kumar. Power control in adhoc networks: Theory, architecture, algorithm and implementation of the compow protocol, 2002.
[14] Samir Das, Charles E. Perkins, Elizabeth M. Royer, and Mahesh K. Markina. Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE Personal Communications, 2008.