Remote Home Security System Based on Wireless Sensor Network Using NS2

#**Rajesh Banala**[1] , Asst.Professor,E-mail: rajesh.banal@gmail.com
#**D.Upender**[2], Asst.Professor, E mail: upender584@gmail.com
#Department of Computer Science and Engineering
SVS Institute of Technology, Warangal, A.P , INDIA

ABSTRACT: ***Nowadays, Wireless Monitoring for home security is among the cutting-edge research area in the field of wireless sensor networks. To implement real-time surveillance of the home security, the intelligent remote monitoring system was developed for home security based on ZigBee technology and GSM / GPRS network. The system can send abnormal images and warning messages through MMS and SMS; receive remote instruction, and remote monitor household appliances. Meanwhile, the introduction of a variety of sensors and the enhancement of system reliability guaranteed that the intelligent remote monitoring system can be responsible for home security. To achieve reliability choosing appropriate routing protocols are essential. This paper presents the simulation results in order to choose the best routing protocol to give the highest performance when the routing protocols like AODV and DSDV are implemented in the target mobile nodes.***

1. INTRODUCTION

Wireless sensor networks (WSN) have critical applications in the scientific, medical, commercial, and military domains. Examples of these applications include environmental monitoring, smart homes and offices, surveillance, and intelligent transportation systems. As social reliance on wireless sensor network technology increases, we can expect the size and complexity of individual networks as well as the number of networks to increase dramatically. Nowadays, securing one's property and business against fire is becoming more and more important. Monitoring commercial and residential areas all-round is an effective method to reduce personal and property losses due to fire disasters. Automatic fire alarm system is widely deployed in those sites recent years. Large numbers of small fire detectors should report their information to the control center of a building or a block. But the cost of wiring is very high in traditional wired fire alarm systems [4].

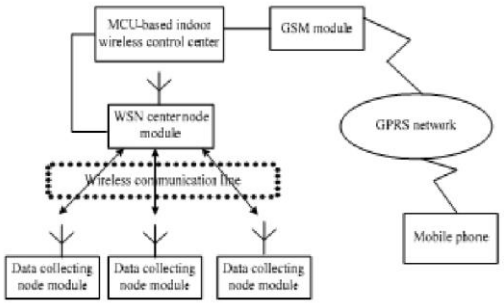

Figure 1: Network Architecture of WSN

Organization of the paper is as follows, section 2 discusses WSN for home security systems, system design and implementation are discussed in section 3, results are discussed in section 4 followed by conclusions.

2. WSN FOR HOME SECURITY SYSTEM

Basically sensor nodes are embedded with transducer, Analog to digital converter, CPU (possibly a microcontroller), communication division, and power supply (possibly rechargeable battery). In sensor networks projects, sensors are deployed in large number in certain geographical area with out intervention of human beings. Because of this, sensor nodes must communicate themselves; pass the information among themselves with in the radio range of the nodes. Hence, sensor nodes are not only used for sensing but also used for communication, for which every node should support sensing and communication. The radio range used in the sensor nodes depends on the sensor network application to be deployed and type of wireless standard used. Most commonly used wireless standards include IEEE 802.11 a/b/g WLAN standards operated under several frequency bands (868MHz, 2.5GHz, 5GHz) are mostly used for higher date transmission rate (preferably for multimedia sensors and at base stations). For short range communication IEEE 802.15.4 Zig Bee standard operated under 868MHz, 915MHz, 2.4GHz ISM band are best suitable (preferable for sensor nodes).

Wireless sensor network is composed of a large amount of miniature self-organizing wireless sensor nodes. By combining three kinds of technology such as sensor, micro-mechatronics and wireless communication [2], WSN can detect, collect and deal with the object information in its covering area, and send data to the observer.

The system structure is illustrated in Figure.1. It is composed of the MCU-based home wireless control center [4], one WSN center node module, and several data collecting nodes, GSM module, GSM network and mobile phone.

In WSN data collecting node modules are connected with pyroelectric infrared detector, temperature sensor, smoke detector and gas sensor separately. When the pyroelectric infrared detector finds that some people intrudes into the house abnormally; or when the temperature sensor detects too high indoor temperature and at the same time [1], the smoke sensor detects over proof smoke concentration; or when the gas sensor detects over proof combustible gas concentration, the sensors will send encoded alarm signal to the home control center through the wireless sensor network established in home. Once the wireless control center receives alarm signal, it will send alarm short message to the users through the GSM module and GSM network immediately**.**

3. SYSTEM DESIGN AND IMPLEMENTATION

3.1 Overview of NS2

Simulation is a very important modern technology. It can be applied to different science, engineering, or other application fields for different purposes. Computer assisted simulation can model hypothetical and real-life objects or activities on a computer so that it can be studied to see how the system function [5]. Different variables can be used to predict the behavior of the system. Computer simulation can be used to assist the modeling and analysis in many natural systems. Typical application areas include physics, chemistry, biology, and human-involved systems in economics, finance or even social science. Other important applications are in the engineering such as civil engineering, structural engineering, mechanical engineering, and computer engineering. Application of simulation technology into networking area such as network traffic simulation, however, is relatively new.

For network simulation, more specifically, it means that the computer assisted simulation technologies are being applied in the

Figure 2: Cluster Architecture

simulation of networking algorithms or systems by using software engineering. The application field is narrower than general simulation and it is natural that more specific requirements will be placed on network simulations. For example, the network simulations may put more emphasis on the performance or validity of a distributed protocol or algorithm rather than the visual or real-time visibility features of the simulations. To simulate the WSN we used a popular open source networks simulator – NS2. Ns-2 is a widely used tool to simulate the behavior of wired and wireless networks. Various types of Wide Area Network (WAN) technologies like TCP, ATM, IP etc and Local Area Network (LAN) technologies like Ethernet, token rings etc., can all be simulated with a typical simulator and the user can test, analyze various standard results apart from devising some novel protocol or strategy for routing etc [8].

3.2 Network Architecture

We simulated the network in NS2 by taking two clusters, each consists of 13 nodes and these clusters contain a cluster head. All the nodes in the cluster have to report the observations to the cluster head so that cluster head in turn will report to the local server (Figure 2). Node 26 is local server and node 27 is surveillance center. The process of routing information from the individual nodes to the cluster head is done by adhoc routing protocols AODV and DSDV.

The simulation is made with the following cases, behavior of the network if nodes in the cluster send the information in a random order and cluster nodes are dead. And the network used is static.

3.3 On-*Demand routing protocols*

In On-Demand routing protocols [6], the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination.

3.3.1 Destination -Sequenced Distance-Vector

The Destination-Sequenced Distance-Vector (DSDV) [7] Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways: a "full dump " or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet[6]. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent.

3.3.2. Ad Hoc on-Demand Distance Vector Routing

AODV [6] is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. It borrows most of the advantageous concepts from DSDV algorithms. The on demand route discovery and usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information. Obtaining the routes purely on-demand [7] makes AODV a very useful and desired algorithm for MANETs.

4. RESULTS

Simulation results are explained in this section. Average values of the entire simulation is given the table 1.From (figure 3) the graph shows there is no

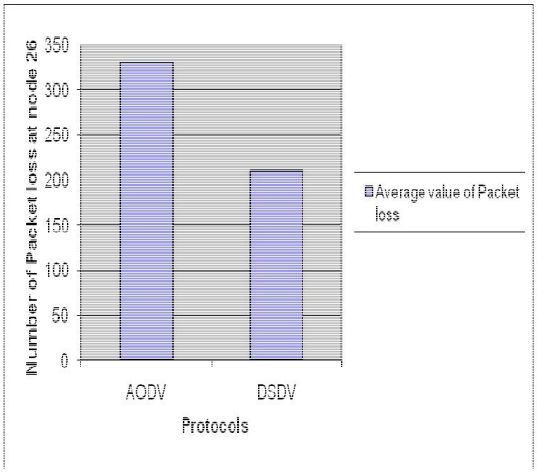

Figure 3: Number of dropped packets at the local server (node 26)

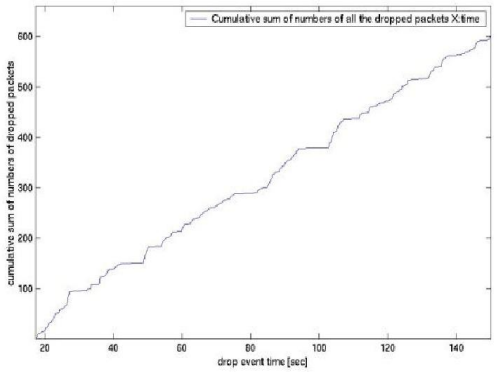

Figure 4: Packet loss in AODV

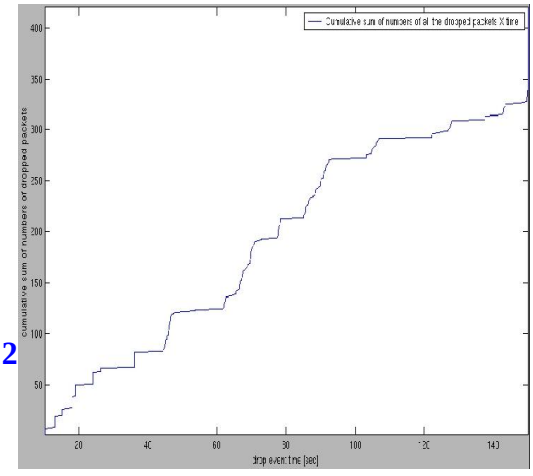

Figure 5: Packet loss in DSDV

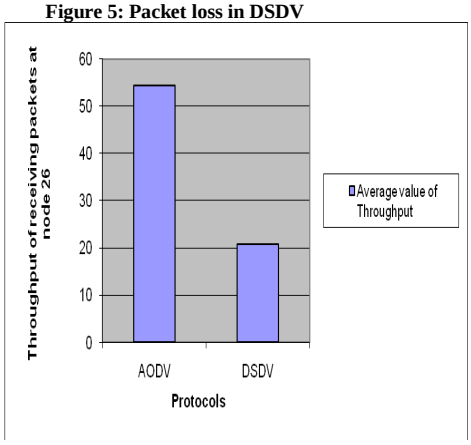

Figure 6:Throughput of receiving packets at the node 26

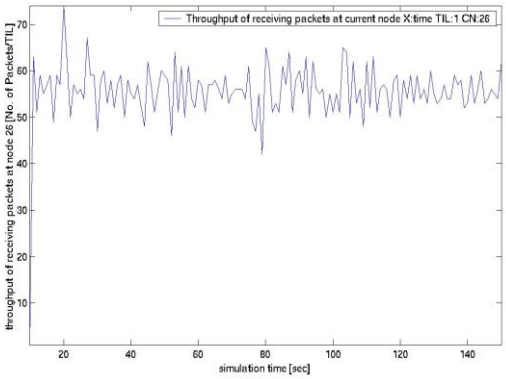

Figure 7:Cluster Throughput in AODV

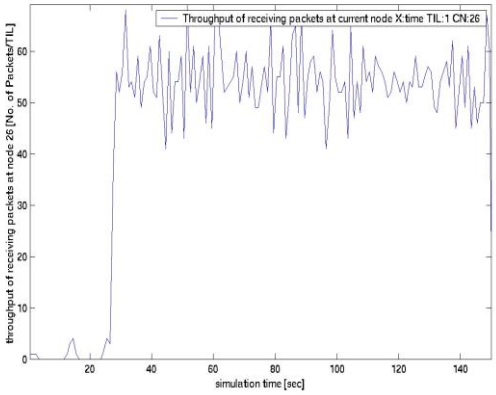

Figure 8:Cluster Throughput in DSDV

much packet loss on DSDV while compare to AODV. This is because when a link fails, a routing error is passed back to a transmitting node and the process repeats. Meanwhile for AODV, this routing protocol shows it is as good as DSDV if packet loss be as indicator. This can be prove by the characteristics of AODV which information on new Routes, broken Links, metric change is immediately propagated to neighbors.

Throughput is a measure of how fast we can send the data through the network.comparision of aodv dsdv using average value of throughput. The explanation of given graph means first we have to take the aodv throughput of receiving packets to 26 node(local center)and same as dsdv throughput of receiving packets to node 36.then we can take average value of throughput choosen.The aodv protocol has less data send to node 26 compare to dsdv so dsdv is the better protocol in the throughput.

This graph implementation first we have to take the every cluster send the packets to the local server (node 26), so that that time the local center how many packets are receive at the random time to check and how many packets are dropped at that time and to draw the packet loss graph of comparison with both AODV and DSDV.

The average packets generated, sent, reveived and dropped values are given in the table 1.

	Routing protocols	Average value of generated packets	Average value of sent packets	Average value of received packets	Average value of dropped packets
Cluster architecture	AODV	4949.5	4944.5	4596.5	430.5
	DSDV	4753.5	4742.0	4191.0	310.5

Table 1: performance analysis of cluster architecture

5. CONCLUSION & FUTURE WORK

The Surveillance system, based on WSN technology, can detect the theft, leaking of raw gas and fire, and send alarm message remotely. The primary contribution of this work is an ex-tended capability in ns-2 to invoke network traffic con-sis tent to the patterns expected for sensor networks. Coordinating these *unique traffic patterns in ns-2 without extensions similar to ours would require very much effort for medium to large networks. Aside from generally increasing the flexibility of ns-2, this work facilitates our objective to evaluate how well current MANET routing protocols support the requirements of various sensor network applications. This paper does the comparison of two routing protocols DSDV and AODV. The significant observation is, simulation results agree with expected results based on theoretical analysis. As expected, reactive routing protocol DSDV performance is the best considering its ability to maintain connection by periodic exchange of information, which is required for TCP, based traffic. In future work a specialized cluster based routing protocol LEACH, LEACH-C can be analyzed.*

REFERENCES

[1] Qiao Qu, Zhao Guohao, Wei Baohua, "Design of Home Safeguard System Based on GSM Technique", Electronic Engineer, vol.32, No.11, pp.76-78, Nov.2006 (in Chinese)

[2] Jin Rencheng, Zhangf Tianchao, "Design and Implementation of Security and Defense System based on GSM", Computer Application, Vol.24 No.12, pp.75-77, Dec. 2004 (in Chinese)

[3] Wu Chengdong, Zheng Jungang, Liu Daren, Xie Kun,
"Study on Smart Home Network Technology Based on Wireless Sensor Network", Academic Journal of Shenyang Jianzhu University, Vol. 21, No. 6, pp.753-756, Nov. 2005 (in Chinese)

[4] Huiping Huang, Shide Xiao, Xiangyin Meng, Ying Xiong, A Remote Home Security System Based on Wireless Sensor Network and GSM Technology, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing.

[5] NS-2, The ns Manual (formally known as NS Documentation) available at *http: //www. isi.edu/nsnam/ns/doc.*

[6] Kapang lego, Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc Network, Indian Journal of Computer Science and Engineering Vol. 1 No. 4 364-371

[7] Nor Surayati Mohamad , Kota Samarahan ,Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009

[8] http://www.wikipedia.org