TRUST PERFORMANCE ANALYSIS IN WIRELESS SENSOR NETWORKS

Dr. M. Pushparani[1], A.Komathi[2]

[1]*Professor and Head, Department. of Computer Science, Mother Teresa Women's University Kodaikanal, Tamil Nadu , (India)*

[2] *Research Scholar, Department. of Computer Science, Bharathiar University, Coimbatore, Tamil Nadu, (India)*

ABSTRACT

Wireless Sensor Networks (WSNs) have their profound applications almost in all possible fields to facilitate automation. All WSNs contain low powered nodes for sensing information about the environmental conditions and incessant reporting to the base station. Secure routing becomes a crucial need as the applications become vital. The nodes must be trust worthy and believable for routing sensed information. Hence I have taken Adhoc On-demand Distance Vector Routing as routing and analyze the various trust parameters packet loss and network through put. Network simulator is used for the simulation study of this protocol.

Index Terms: Communication, Trust, Multihop, Wireless Sensor Network, Performance Analysis

I. INTRODUCTION

Wireless sensor networks (WSNs) are low powered devices that are incorporated in various application fields to report sensed information to the base station. It consists of spatially distributed autonomous sensors to monitor physical or environmental conditions like temperature, sound, pressure, etc. In addition, it cooperatively passes data through the network to a main location. The prevailing networks considered here communicate in a multihop manner, control and coordinate network constraints.

The main operation of a network is data transfer. To facilitate communication between the network nodes, a proper establishment of path between source and destination nodes is necessary. This is achieved with the help of a routing protocol. Routing in WSNs is a very challenging task due to their unique characteristics, dynamic nature, architecture/design issues and resource constraints. A routing protocol is responsible for efficient performance of a data transfer function.

II. WIRELESS SENSOR NETWORK

Individual sensor nodes in a WSN are inherently resource-constrained. They have limited processing capability, storage capacity, and communication bandwidth. Each of these limitations is due in part to the two greatest constraints—limited energy and physical size.

Energy: Energy consumption in sensor nodes can be categorized into three parts:

-Energy for the sensor transducer; Energy for communication among sensor nodes; and

-Energy for microprocessor computation.

Computation: The embedded processors in sensor nodes are generally not as powerful as those in nodes of a wired or ad hoc network.

Memory: Memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate computations. There is usually not enough space to run complicated algorithms after loading OS and application code.

Transmission range: The communication range of sensor nodes is limited both technically and by the need to conserve energy. The actual range achieved from a given transmission signal strength is dependent on various environmental factors such as weather and terrain.

III. LITERATURE SURVEY

According to the literature there is a classification of the trust based protocols and strategies, Trust is divided into centralized, distributed and hybrid trust.

3.1 Centralized Trust Management

Centralized trust mechanisms have a single entity that evaluates the trust of a node while routing information from S to the BS. Reputation systems seek to restore the shadow of the future to each transaction by creating an expectation that other people will look back upon it [2]. The keynote trust management system also depicts a centralized trust mechanism introduced in [3].

3.2 Distributed Trust Management

Distributed Trust Management schemes are techniques in which the nodes individually estimate the trust values of their immediate neighbours, forwarders, receivers and passerby nodes (if mobility is also present) [4] and [5].

3.3 Hybrid Trust Management

Hybrid trust management (HTM) schemes (e.g. [6, 7]) contain the properties of both centralized as well as distributed trust management approaches. The main objective of this approach is to reduce the cost associated with trust evaluation as compared to distributed approaches. This scheme is used with clustering schemes, in which cluster-head acts as a central server for the whole cluster.. It introduces more communication overhead in the network as compared to the distributed one.

Jamal N. Al-Karaki et al., [8] discussed the challenges in the main design of WSN to carry out data communication. The design of routing protocols in WSNs is influenced by many challenging factors like Node deployment , Energy consumption without losing accuracy , Data Reporting Model, Fault Tolerance etc. These factors must be overcome before efficient communication can be achieved in WSNs

IV. AD HOC SYSTEM

The one proposed routing system is Ad hoc On-Demand Distance Vector routing. The trust establishment between nodes is a must to evaluate the trustworthiness of other nodes, as the survival of a WSN is depends on the cooperative and trusting nature of its nodes.

This proposed routing source floods a route request message (RREQ) and obtains a route reply (RREP) on the availability of routes. On the occurrence of any link failure, the node sends a route error message (RERR) to the source and the transmission is begun all over again.

Trust in AODV

The proposed metric to evaluate the trust in this protocol is given in equation (1) below.

: Trust check = (Forwarding Capability + Reputation + Frequency of use) / total number of nodes. (1)

Figure 2 shows the checked trust of this protocol.

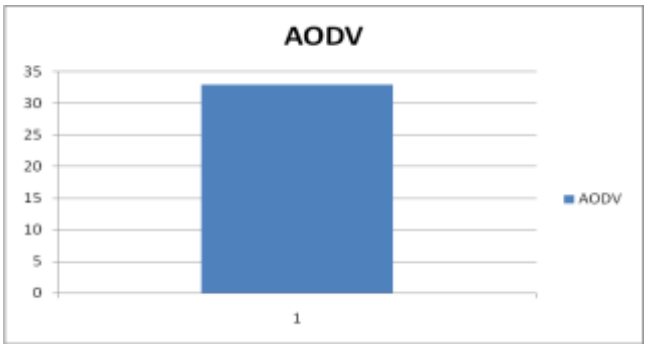

Fig. 2. Trust in AODV

V. SIMULATION ANALYSIS

Network Simulator (NS) is a simulation tool targeted at both wired and wireless (local and satellite) networking research. NS is a very promising tool and is being used by researchers. To analyze the efficiency of AODV the parameters in Table 1 are used in the network simulator.

Table.1 Simulation Parameters

Parameter	Value
Simulation Time	30 ms
Number of nodes	50
Routing protocol	AODV
Traffic model	CBR
Simulation Area	800 x 800
Transmission range	250m
Antenna Type	Omni antenna
Mobility model	Two ray ground
Network interface Type	WirelessPhy

5.1 Network Throughput

Throughput means the number of packets delivered successfully in a network. Throughput is plotted in figure 4.

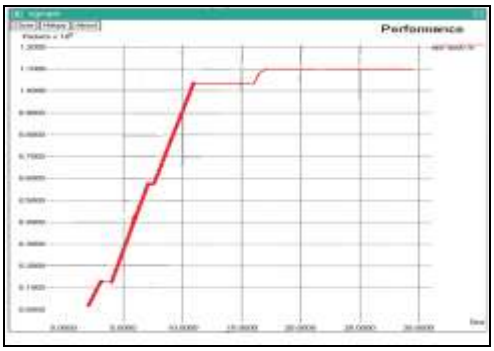

Fig. 1. Throughput of AODV

5.2 Packet Loss

Packet loss is the total number of packets lost during communication. Figure 5 shows that the total packets lost by AODV protocol.

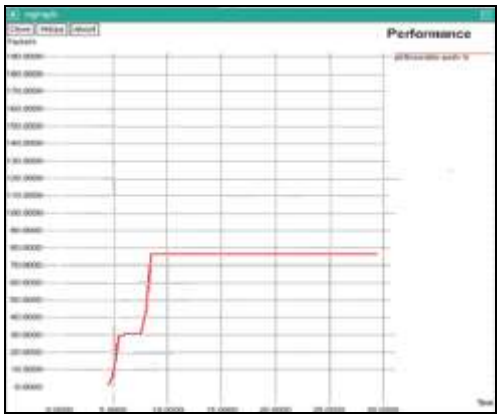

Fig. 2. Packet Loss of AODV

VI. CONCLUSION

The design, simulation and analysis of the Trust checking in AODV are analyzed in this paper. The through put and packet loss are analyzed . Future works can find out the security in this protocol and see how it responds to various attacks and energy variations in a WSN.

REFERENCES

[1] Momani, Subhash Challa, Survey of Trust Models in Different Network Domains , Melbourne, Australia.

[2] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems: Facilitating trust in internet interactions.Comm. of the ACM, 43(12):45–48, 2000.

[3] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytics. The keynote trust management system. In RFC2704, 1999.

[4] Saurabh Ganeriwal and Mani B. Srivastava. Reputation-based framework for high integrity sensor networks. In Proc. of ACM Security for Ad-hoc and Sensor Networks, October 2004.

[5] Azzedine Boukerche, Xu Li, and K. EL-Khatib. Trust-based security for wireless ad hoc and sensor networks. Computer Comm., 30:2413–2427, September 2007.

[6] Riaz Ahmed Shaikh, Hassan Jameel, Sungyoung Lee, Saeed Rajput, and Young Jae Song. Trust management problem in distributed wireless sensor networks. In Proc. of 12th IEEE Int. Conf. on Embedded Real Time Computing Systems and its Applications, pages 411–414, Sydney, Australia, August 2006.

[7] K. Krishna and A. bin Maarof. A hybrid trust management model for mas based trading society. The Int. Arab Journal of Information Technology, 1:60–68, July2003.

[8] Jamal N. Al-Karaki Ahmed E. Kamal Routing Techniques in Wireless Sensor Networks: A Survey