International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 3, Issue 6
June 2015.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

COMPARATIVE STUDY OF AODV, DSR AND DSDV IN WNS

D.Prasanna[1], J.Raja[2]
[1,2]Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

Abstract:

Wireless Sensor Networks (WSNs) have their significant applications nearly in every conceivable field to encourage mechanization. All WSNs contain low fueled hubs for detecting data about the natural conditions and unending answering to the base station. Security is an extremely basic and basic criterion for correspondence. The hubs must be trust commendable and authentic for steering detected data. Thus we investigate the dependability of AODV, DSR and DSDV conventions in a WSN. Organize test system is utilized for the reenactment examination of the three conventions.
Keywords: Communication, wireless sensor network, trust, multi-hop, performance analysis.

Introduction

Wireless sensor networks (WSNs) are low fueled gadgets that are consolidated in different application fields to report detected data to the base station. Late years have demonstrated an uncommon capacity to watch and control the physical world, nonetheless, as with practically every innovation; the advantages of WSNs are joined by a huge hazard elements and potential for mishandle [1]. In the event that WSN operations fall flat or on the off chance that they are deferred, as it were, then the entire reason for the system perishes.

Attributable to the way of WSN organization being inclined to the encompassing condition and experiencing different sorts of assaults notwithstanding the assaults found in customary systems, other security estimations not quite the same as the traditional methodologies must be set up to advance the security of the system The trust foundation between hubs is an unquestionable requirement to assess the reliability of different hubs, as the survival of a WSN is depends on the cooperative and trusting in nature of its nodes. The remaining section of the paper is like this: literature survey; trust in AODV, DSDV, DSR protocols.

Related Survey

Some of the trust evaluation strategies are discussed in this section. Trust is the factor that is used to test the calibre of a node in terms of whether it is good enough to perform its corresponding tasks.

According to the literature there is a classification of the trust based protocols and strategies, which is shown in figure 1. Trust is divided into centralized, distributed and hybrid trust.

Centralized Trust Management

Trust instruments have a solitary element that assesses the trust of a hub while directing data from Source to the Basestation. Reputation frameworks seek to reestablish the shadow of the future to each by making a desire that other individuals will think back upon it [2].

The keynote trust management system additionally depicts a centralized trust component presented in [3].

Distributed Trust Management

Disseminated Trust Management plans are systems in which the hubs independently assess the trust estimations of their prompt neighbors, forwarders, collectors and passerby hubs (if versatility is likewise present) [4] and [5].

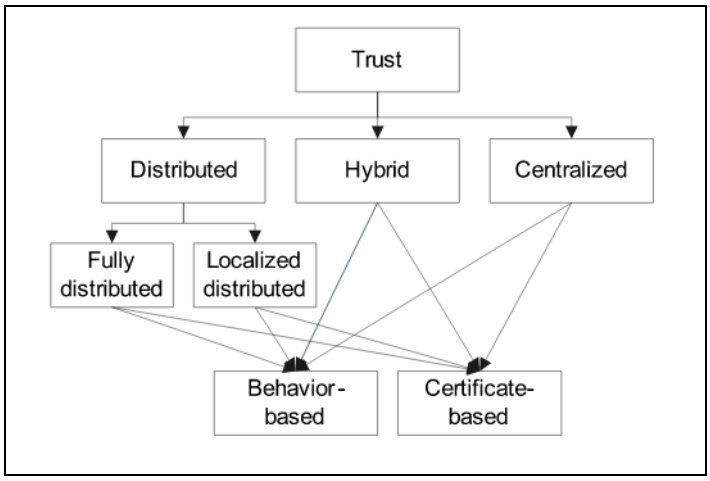

Figure.1 Categorization of Trust

Hybrid Trust Management

Hybrid trust management (HTM) methods (e.g. [6, 7]) include the properties of both integrated and in addition conveyed trust administration approaches. The essential target of this approach is to reduce the cost connected with trust assessment when contrasted with disseminated approaches. This preparation is utilized with grouping plans, in which bunch head goes about as a focal server for the entire bunch. It presents more association overhead in the framework when distinguished among the circulated one.

Trust in AODV, DSDV, and DSR protocols

The working of the three protocols is different from each other and this will have a great impact on the trust.

AODV

In Ad hoc On-Demand Distance Vector routing, a source floods a route request message (RREQ) and obtains a route reply (RREP) on the availability of paths. The occurrence of any link drops, the node sends a route error message (RERR) to the source and the transmission is begun all over again.

DSDV

In Destination Sequenced Distance Vector (DSDV) routing, all hubs proactively keep up a steering table and utilize these courses in view of the succession numbers for directing operations. This protocol is said to deliver a decent measure of overhead while routing.

DSR

In Dynamic Source Routing (DSR), the hubs likewise perform source based directing, the best distinction being the supply of courses from the store memory of the hubs to accelerate the steering procedure. Also the route maintenance mechanism in the DSR protocol is noteworthy.

Trust in AODV, DSDV and DSR

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

$$\text{Trust check} = (\text{Reputation} + \text{Forwarding Capability} + \text{Frequency of use}) / \text{total number of nodes} \quad (1)$$

To estimate which of the three protocols has the highest trustworthiness we evaluate (1) for the network scenario in table 1. Figure 2 shows the comparison of the checked trust in the three protocols.

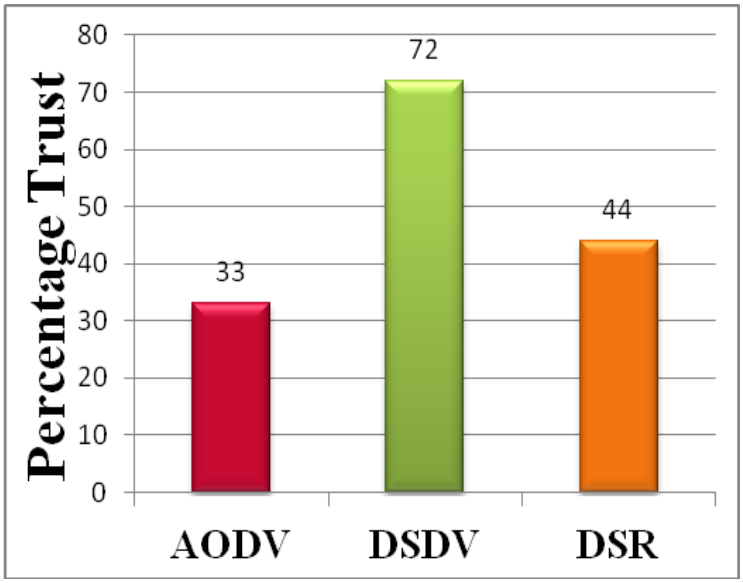

Figure.2 Comparison of Trust in AODV, DSDV and DSR

Simulation Analysis

Network Simulator (NS2) is a simulation tool targeted at both wired and wireless (local and satellite) networking research. NS is an exceptionally encouraging instrument and is being utilized by scientists. To examine the effectiveness of AODV, DSDV and DSR, the parameters in Table 1 are utilized as a part of the system test system.

Simulation Parameters

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

Network Throughput

Throughput implies the quantity of parcels conveyed effectively in a system. For AODV, DSDV and DSR,the throughput is plotted in figure 3. Clearly the throughput is higher for DSDV in our investigation.

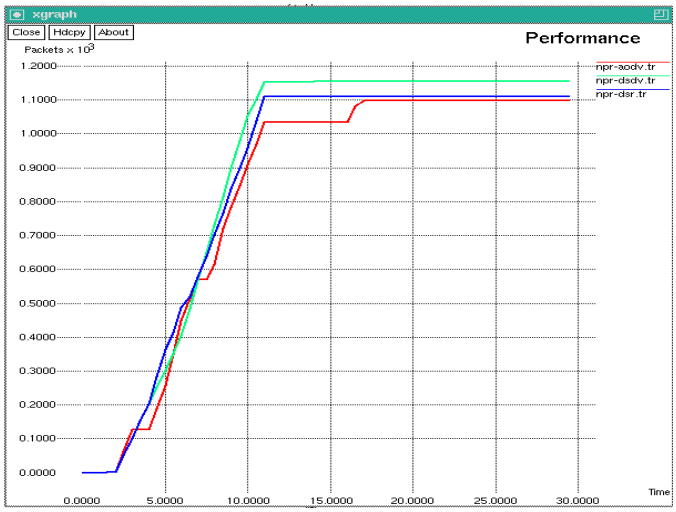

Figure.3 Throughput of AODV, DSR and DSDV

Packet Loss

Packet loss is the total number of packets lost during communication. Figure 4 shows that the total packets lost by AODV protocol is much lesser when compared with the the other protocols

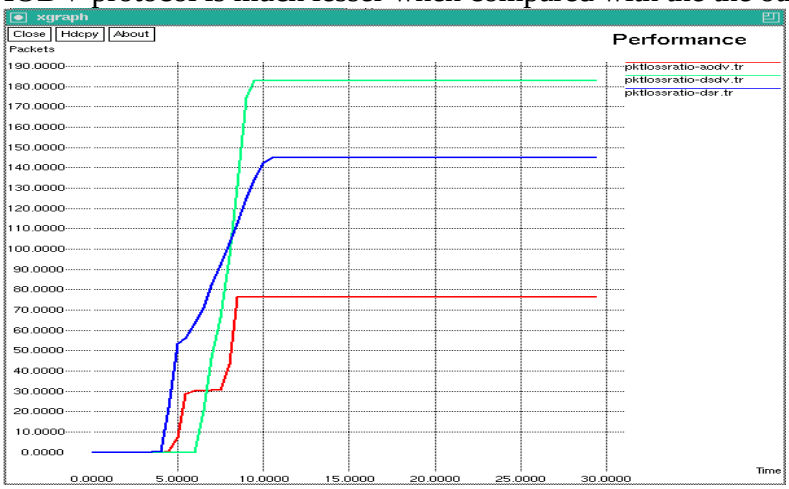

Figure.4 Packet Loss of AODV, DSR and DSDV

Conclusion

The design, simulation and analysis of the Trust checking in AODV, DSDV and DSR protocols are shown in this paper. The underlying order of trust gives and understanding into the current plans. We can finish up from this reenactment investigation that DSDV is more dependable. In spite of the fact that DSDV causes all the more overhead, which is the reason more parcels are lost, as far as trust it is a proficient convention. This is a direct result of the proactive way of the convention.

Reference

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

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

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

[6]. Hassan Jameel, Sungyoung Lee, Riaz Ahmed Shaikh, Saeed Rajput, and Young Jae Song. Trust management problem in distributed wireless sensor networks. In Proc. of 12th IEEE Int. Conf., 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.