ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Performance Evaluation of Routing Protocols for Anomaly Detection

Rani.T.P1, JayaKumar.C2

Research Scholar, Anna University, Chennai, India

R.M.K.Engineering College, Chennai, India

Abstract: Wireless sensor network is a data centric network consisting of a number of sensor nodes that work cooperatively to form an infrastructure less network. The sensing technology combined with processing power and wireless communication makes it being available for a number of futuristic applications. Anomalies in Wireless sensor networks coerce it to perform denial of service. Anomaly detection plays a vital role in securing a network from obliteration. Anomaly detection addresses a detection technique based on Hypothesis testing. It performs the detection technique using routing protocols such as AODV, DSDV and DSR and network performance is analyzed. It concludes that DSR has better performance with some tradeoffs when compared to the other routing protocols we analyzed.

I INTRODUCTION

Wireless sensor network (WSN) consists of a number of sensor nodes that work in cooperation with each other to perform event monitoring, data collection and filtering [1, 2, 3]. In Recent years WSN has gained its importance because of its wide range of applications like Structural monitoring, Bio-habitat monitoring, Industrial monitoring, Disaster management, Military surveillance, Home or building security system, Video Surveillance and so on [1]. They are used to monitor Temperature, Pressure, Volume, Density and various parameters and execute task related to these parameters. There are various issues and challenges in WSN. As sensor nodes are deployed in distributed environment, there are various security threats in WSN [4, 5, 6, 7]. The WSN can be prone to many security attacks. Some general security attacks [4, 5, 6, 7] in WSN are Sybil Attack [8], Clone Attack [9], Sink hole attack [10] and Worm hole attacks [11]. As in any networks, confidentiality, availability, authenticity and integrity are primary goals of security in WSN [5].

Anomaly is an erroneous data transmission [12, 13, 14, 15, 16]. It is a measurement that deviates from the other data in a data set. There are various sources of anomalies such as internal and external sources [15]. Sensor nodes have limited computation and communication capabilities. Due to its limitations of power and resources it may produce erroneous data. As sensor nodes are deployed in harsh environments it may be affected by noise or malicious user or node may tamper and it may create such a data. If such a deviated data is transmitted and data aggregation is performed resultant data may not be accurate [18, 19].

There are various existing data aggregation mechanisms [17] such as Statistical based approaches [20], nearest neighbor Based approaches [21], Clustering based approaches [22], and Classification based approaches [23].

In this paper we propose a statistical based approach for anomaly detection. We assume that the base station cannot be tampered and all sensor nodes send data to head node. The nodes once created communicate with head node through routing protocols [24, 25, 26, 27, 28]. The head node forwards it to base station. The head node sends only the authenticated data to the base station. Thereby guarantying security of data sent. The base station fixes the threshold values for measuring the deviation in data. We compare the Routing protocols such as Adhoc On Demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV) and Distance Vector Routing Protocol (DSR) for Anomaly detection.

The rest of the paper is organized as follows. We present the literature survey as related works in Section II. In this section survey about the existing protocols in WSN is done. In Section III we proceed with the implementation of our algorithm. We explain the simulation and comparative results in Section IV and conclusion is given in Section V.

II RELATED WORKS

A study of secure communication in WSN was earlier made and the work was presented as an initial version in [7]. A study on routing protocols and results were made and they are discussed as follows. Routing Protocols are mainly classified as Table Driven [24] and On demand [25]. Table driven protocols initiates a node to maintain details about routes, at the time of creation of node and updates the details periodically. It sends entire details to its neighbors and propagates the details by flooding. They are also called as Pro Active Routing Protocols [25]. Routing Protocol DSDV is an example for Table Driven. On demand Routing Protocols detect a route to destination node as per requirement. The source node broadcast Route request and gets Route reply as a uni- cast message. The route reply contains the entire route information through which the Route request message had traversed. DSR is such an example. Another example Routing Protocol AODV is similar to DSR, but the Route reply does not contain the entire message. Instead it carries the next hop information and traverses to the source. They are also called as Reactive Routing Protocols [26]. Hybrid routing protocols [26] combine the principle of Table driven and On demand Routing Protocol. Zone Routing Protocol ZRP [26] is an example for Hybrid Routing Protocol.

Protocol comparison based on study of Routing Protocols is summarized in Table 2.1

Table 2.1

Comparative study of Routing Protocol

Protocol Property	AODV	DSDV	DSR
Loop free	Yes	Yes	Yes
Multicast	No	No	Yes
Periodic Broadcast	Yes	No	Yes
Routes	Routing	Routing Table	Routing
Maintained	Table	Cache	Table
Proactive	Yes	No	No

III ANOMALY DETECTION

We assume that the Base Station is powerful such as a laptop or a wireless system which is capable of complex computation. Cluster formation is assumed to be done using any one of the cluster algorithms. The head node of a cluster transfers data to the base station. The Base station on receiving the datum from the head nodes performs the following steps for anomaly detection using threshold comparison. We have used MD5 algorithm for authentication [29]. The algorithm steps for anomaly detection are given in Fig 3.1.

Fig 3.1 Algorithm to find data anomaly

1. Check whether the datum is authenticated. For authentication MD5 algorithm is used.
2. Check Whether $D<Th_{min}$. If so declare it as an anomalous data.
3. Check Whether $D> Th_{max}$. If so declare it as an anomalous data.
4. Declare the details of Anomalous node to all nodes through flooding.
5. Perform data aggregation on all correct data obtained finding the sum of all data and calculate approximate data.

The head node accepts a data from a sensor node only if it satisfies the following condition. We assume the Network packets to be transmitted using Drop Tail Queue [30].

The algorithm has a time complexity [30] of O(1) despite of the number of nodes in a network as it involves data aggregation.

The assumptions and requirements for data is given in Fig 3.2.

IV PERFORMANCE EVALUATION

The detection technique is implemented using NS2 simulator [31, 32, 33]. We have chosen NS2 as it is an open source event driven simulator specially designed for researchers in computer communication networks. The algorithm is implemented at the head node. We compare the performance of different routing

protocols such as AODV, DSDV and DSR. Traffic and mobility model based on Constant Bit Rate (CBR) is used [34]. The field configuration used is 1500m x 1500m. The parameters that have been considered for simulation of comparative study about routing protocols to implement anomalous detection are given below in Table 4.1.

Fig 3.2 Assumptions and Conclusions

Let D be the data set where D→ w, w is a set all natural numbers, i.e {1,2,..n}
d is the data sent by sensor node.
d is a subset of D
P(d) and Q(d) are propositional statement which states that
P(d) :d>Thmin and Q(d): d<Thmax
Accept d if it satisfies the following condition.

d€D: P(d) ∧ Q(d) (∃dD: P(d) ∧ ∃dD: Q(d)

Table 4.1 Simulation Parameters

Parameter	Value
Protocols	AODV, DSDV, DSR
Traffic Source	Constant bit rate (CBR)
Simulation Time	200 s
Packet Size	512 bytes
Queue	Drop Tail
Area	1500m x 1500m
No: of nodes	40,50,60,70 and 80
Pause Time	10,20,30,40,50,60 and 70
Maximum Speed	10,20,30,40,50,60 and 70
Mobility Model	Random Way Point

In order to evaluate our algorithm using various routing protocols the following metrics [32] were considered.

Packet Delivery Ratio [32] is the ratio of total number of packets successfully delivered and total number of packets generated. Increase in Packet Delivery Ratio indicates increase in successful packet transmission.

AODV has higher and constant Packet Delivery Ratio when compared to other protocols pertaining to increase in the number of nodes.

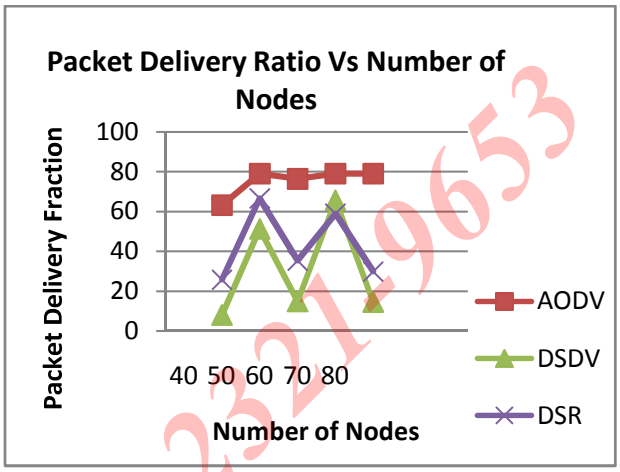


Fig 4.1 Packet Delivery Ratio Vs Number of Nodes

The End to end delay [32] indicates the total delay incurred in transmitting a packet such as route discovery latency, queuing or intermediate buffering, re-transmission at MAC, propagation and transmission delays. The average of End to end delay is the average end to end delay. Simulation is run several times and its average is found.

End to End Delay = (Arrival Time – Send Time) / ∑ No. of connections

Average End to End Delay = ∑ End to End delay / ∑ No. of simulations conducted

DSR has the highest average end to end delay. DSDV has a low and it maintains a constant delay despite of an increase in the number of nodes. AODV shows a variation in delay.

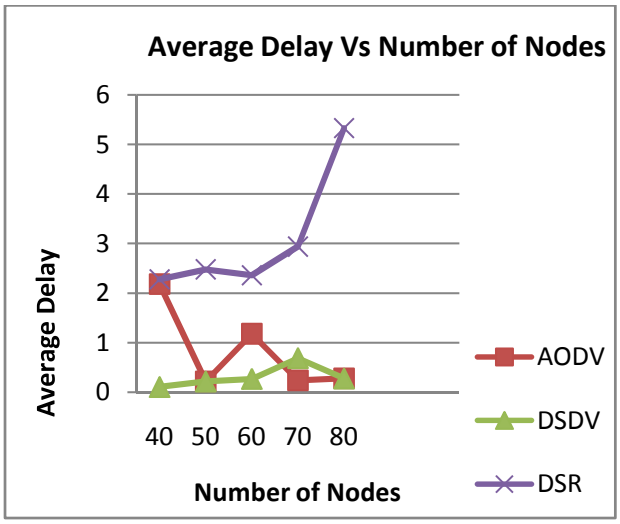


Fig 4.2 Average Delay Vs Number of Nodes

Jitter [32] is the measure of variation in delay between the arrivals of packets of a particular node.

Jitter = Previous Packet delay- Current Packet Delay

AODV shows a maximum value of Jitter and it maintains it on an average high value. DSDV and DSR have very low and almost same and constant value of Jitter.

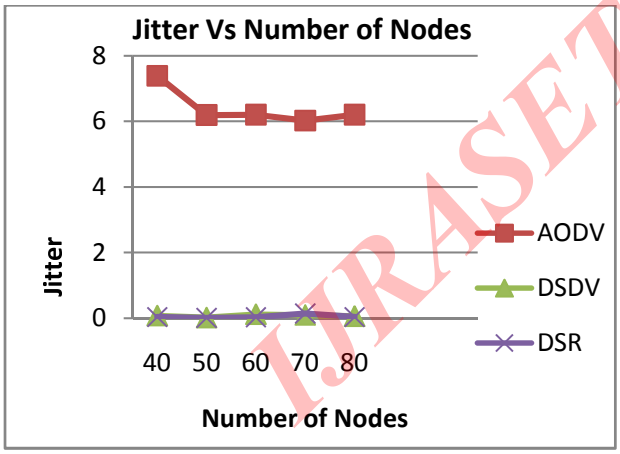


Fig 4.3 Jitter Vs Number of Nodes

Throughput [32] is the total number of bits received at an end per second.

Throughput = ∑ No. of bits received per second

AODV has the minimum throughput when compared to DSDV and DSR.

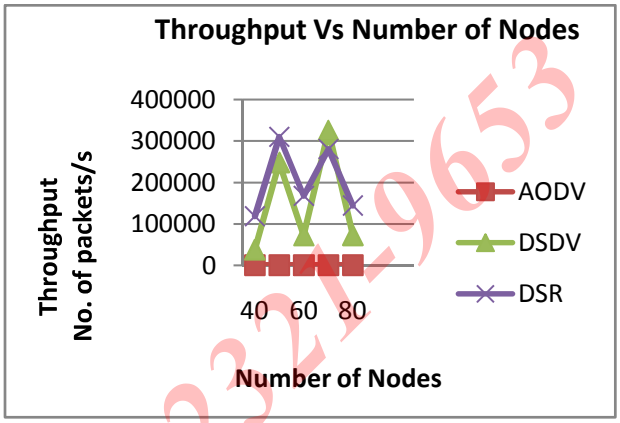


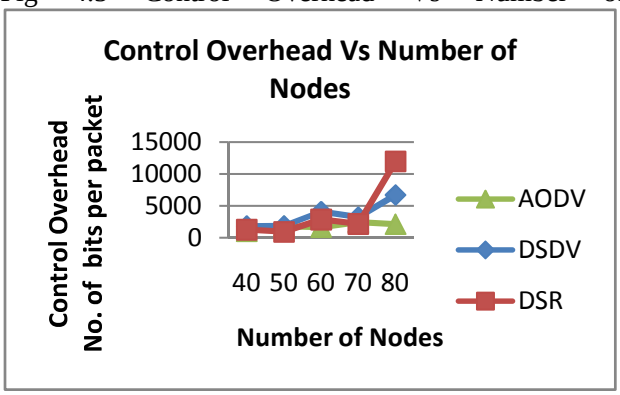
Fig 4.4 Throughput Vs Number of Nodes

Overhead [32] is the cost involved in transmitting a packet. It is calculated in terms of time for transmission.

Control Overhead [32] is the Overhead involved in transmitting non data packets. They are used for network maintenance purpose. Normalized routing Overhead is the cost involved in data transmission.

AODV has significantly higher control and normalized overhead when compared to DSDV and DSR.

Fig 4.5 Control Overhead Vs Number of Nodes



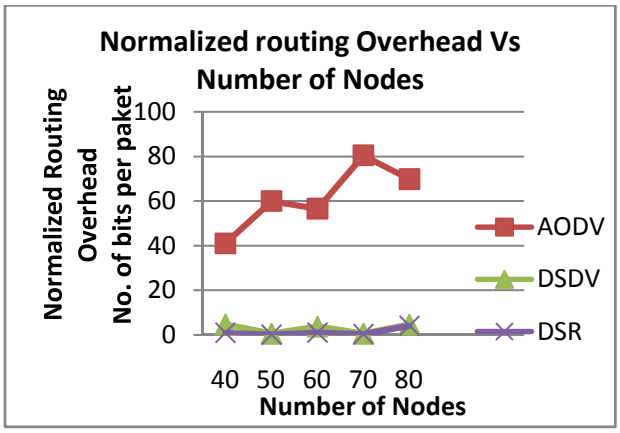


Fig 4.6 Normalized routing Overhead Vs Number of Nodes

An Increase in Pause Time [32] means lower mobility. Similarly an increase in Maximum speed [32] means higher mobility. The increase in mobility may cause frequent link failures. The working mechanism of routing protocols gives varying results

While varying Pause Time, AODV has the least throughput and shows a significant increase in Overhead and Jitter. AODV has the maximum Packet Delivery Ratio and hence when pause time of nodes is varied, AODV show significant differences. But the increase in Overhead and Jitter and decrease in throughput makes DSR to be a better option for AODV. The following are the visual results of the performance metrics with respect to the varying Pause time.

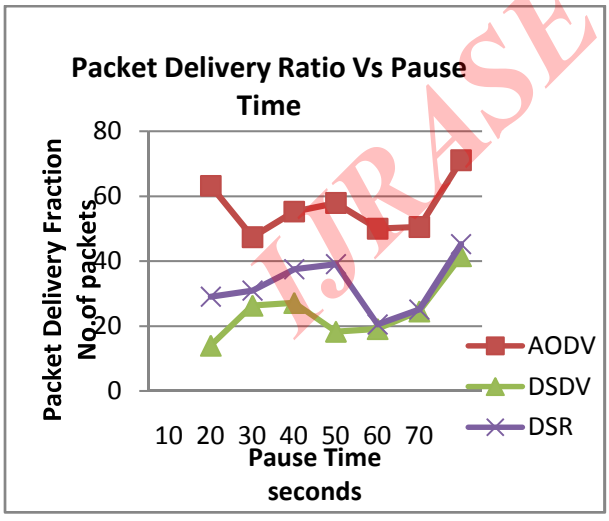


Fig 4.7 Packet Delivery Ratio Vs Pause Time

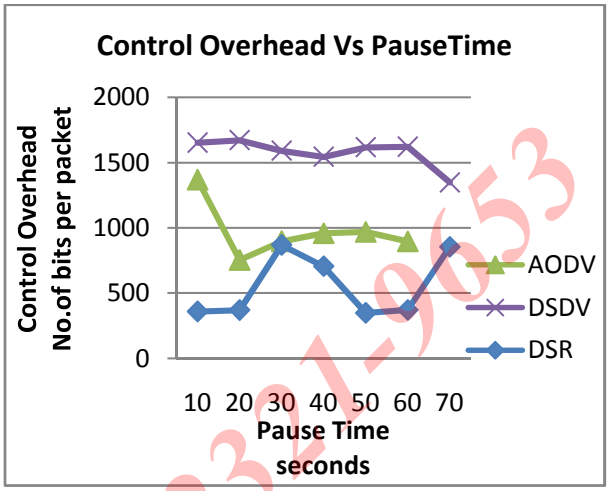


Fig 4.8 Control Overhead Vs Pause Time

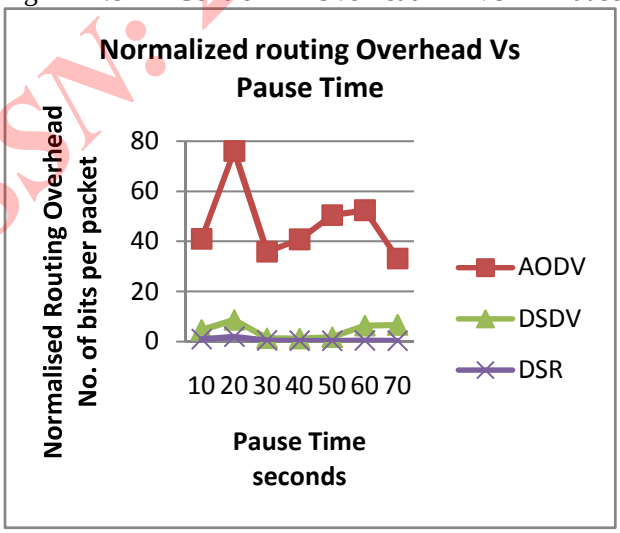


Fig 4.9 Normalized Overhead Vs Pause Time

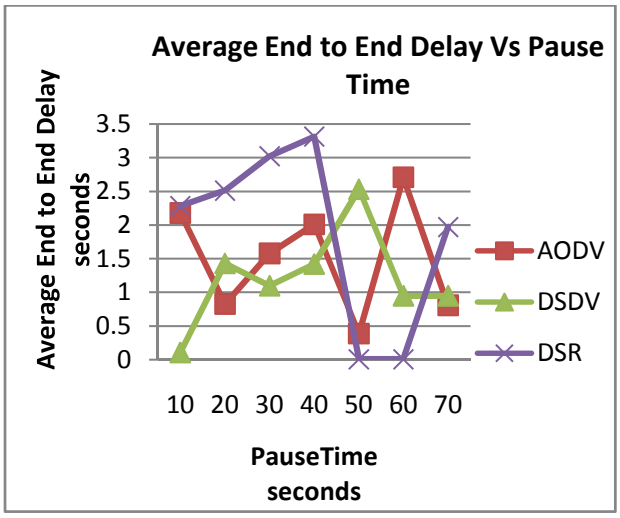


Fig 4.10 Delay Vs Pause Time

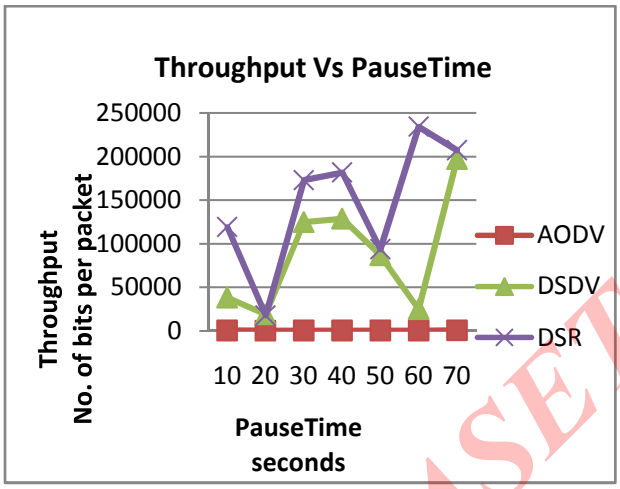


Fig4.11Throughput Vs Pause Time

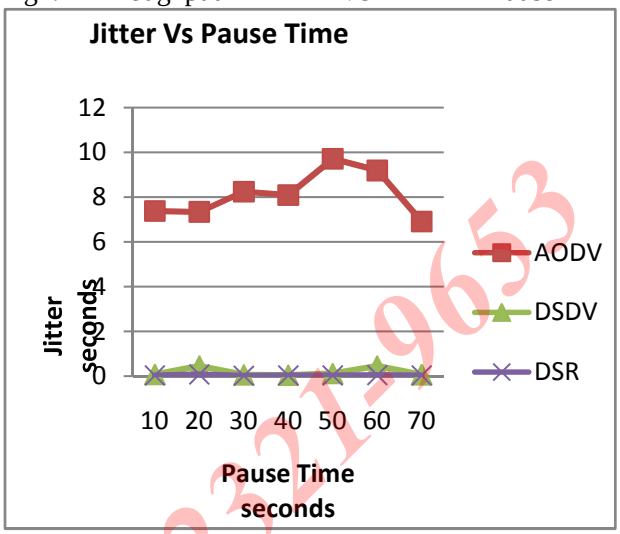


Fig 4.12 Jitter Vs Pause Time

V CONCLUSION

Based on these performance metrics AODV has maintained low throughput although packet delivery fraction is maintained as high. Comparing DSDV and DSR, they have similar pattern for throughput and Packet delivery Fraction. But when we compare them with metrics like Jitter and Average End to End Delay, DSR has high Average End to End Delay. Both protocols maintain similar Normalized routing Overhead. So we claim that DSR can be a better protocol in wireless sensor networks performing a particular task in terms of Packet Delivery Ratio and Throughput. Since the Average End to End Delay is higher there has to be trade off while introducing these protocols in Wireless Sensor Networks.

REFERENCES

[1] Akyildiz.W.Su,Y.Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] Holger Karl, Andreas Willig, “Protocols and Architectures for Wireless Sensor Networks", John Wiley, 2005.

[3] Kazem Sohraby, Daniel Minoli, & Taieb Znati, "Wireless Sensor Networks- Technology, Protocols, and Applications", John Wiley, 2007.

[4] Pathan, A.K, Kyung Hee Univ, Seoul, Hyung-Woo Lee, Choong Seon, "Security in wireless sensor networks: issues and challenges", in Proc. 8th International Conference on Advanced Communication Technology ICACT 2006, vol.2, pp.1048-1053,2006.

[5] Xiaojiang Du , Fargo, Hsiao-HwaChen "Security in wireless sensor networks", IEEE Wireless Communications, vol.15, no.4, pp. 60-66, Aug 2008.

[6] Martins.D, Guyennet.H, Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey, in Proc. International Conference on Network-Based Information Systems (NBiS), pp.313 – 320, Sept. 2010.

[7] T.P.Rani, Dr.C.JayaKumar(2012), Establishment Of Secure Communication In Wireless Sensor Networks, Computer Science & Engineering: An International Journal (CSEIJ), vol.2, no.2, pp.35-39.

[8] Palanisamy.V, Annadurai.P, VijilakshmiS, "Curbing and curing sybil attack in ad hoc network", in Proc. International Conference on Advanced Computing, ICAC, pp. 1-5, Dec 2009.

[9] Sathish.R, Kumar.D.R, "Dynamic Detection of Clone Attack in Wireless Sensor Networks", in Proc. International Conference on Communication Systems and Network Technologies (CSNT), pp.501-505, April'2013.

[10] Krontiris.I, Giannetsos.T, Dimitriou.T, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side", in Proc. IEEE International Conference on Wireless and Mobile Computing, WIMOB'08, pp.526 – 531, Oct. 2008.

[11] Farid Naït Abdesselam, Brahim Bensaou, Tarik Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Adhoc Networks", IEEE Communications Magazine, pp.127-133, April 2008.

[12] http://en.wikipedia.org/wiki/Outlier

[13] Yang Zhang, Nirvana Meratnia, and Paul Havinga, "Outlier Detection Techniques for Wireless Sensor Networks: A Survey", IEEE communications surveys & tutorials, vol. 12, no. 2, second quarter 2010.

[14] Weiyu Zhang, Qingbo Yang, Yushui Geng, "A Survey of Anomaly Detection Methods in Networks", in Proc. International Symposium on Computer Network and Multimedia Technology, vol.2, no. 1, pp. 01-03, Jan. 2009.

[15] Varun Chandola, Arindam Banerjee, "Anomaly Detection for Discrete Sequences: A Survey", IEEE Transactions On Knowledge And Data Engineering, vol.24, no. 5, May 2012.

[16] Jingke Xi, XuZhou, Jiangsu, "Outlier Detection Algorithms in Data Mining", in Proc. Second International Symposium on Intelligent Information Technology Application, vol. 1, pp. 94-97, Dec 2008.

[17] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", IEEE Transactions On Information Forensics And Security, vol. 7, no. 3, pp.1040-1052, June 2012.

[18] Mo Li, XiaoHua Xu ; ShiGuang Wang ; Shaojie Tang ; Guojun Dai ; Jizhong Zhao ; Yong Qi, "Efficient data aggregation in multi-hop wireless sensor networks under physical interference model", in Proc. IEEE 6th International Conference on Mobile Adhoc and Sensor Networks, pp. 353-362, 2009.

[19] Chi-Tsun Cheng, Chi K. Tse, "A Delay-Aware Network Structure for Wireless Sensor Networks with Consecutive Data Collection Processes", IEEE Sensors Journal, vol.13, no.6, June 2013.

[20] Hyuntea Kim, Jaebok Park, Giwhan Cho, "Statistical Data Aggregation Protocol Based on Data Correlation in Wireless Sensor Networks", in Proc. International Coneference on Information Technology Convergence, ISITC 2007, pp. 130 – 134, Nov. 2007.

[21] Tossapon, Boongoen and Qiang Shen, "Nearest-Neighbor Guided Evaluation of Data Reliability and Its Applications", IEEE Transactions on Systems, Man, and Cybernetics, vol. 40, no. 6, December 2010

[22] Woo-Sung Jung,Keun-Woo Lim, Young-Bae Ko, Sang-Joon Park, "A Hybrid Approach for Clustering Based Data Aggregation in Wireless Sensor Networks", in Proc. ICDS '09. Third International Conference, pp. 112 – 117, Feb 2009.

[23] Bokareva.T, Bulusu.N, Sanjay Jha, "Graph theory based aggregation of sensor readings in wireless sensor networks", in Proc. 33rd IEEE Conference on Local Computer Networks, pp. 514-515, Oct 2008.

[24] Patil.M, Biradar.R.C, "A survey on routing protocols in Wireless Sensor Networks", in Proc. 18th IEEE

International Conference on Networks (ICON), pp. 86-91, Dec'2012.

[25] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das and Mahesh K. Marina, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks", IEEE Personal Communications, vol. 8, no. 1, pp. 16-28, Feb'2001.

[26] Md. Arafatur Rahman and Farhat Anwar, Jannatul Naeem and Md. Sharif Minhazul Abedin, "A Simulation Based Performance Comparison of Routing Protocol on Mobile Ad-hoc Network (Proactive, Reactive and Hybrid)", in Proc. International Conference on Computer and Communication Engineering (ICCCE 2010), pp. 11-13, May 2010.

[27] Murizah Kassim, Ruhani Ab. Rahman, Roihan Mustapha, "Mobile Ad Hoc Network (MANET) Routing Protocols Comparison for Wireless Sensor Network", in Proc. IEEE International Conference on System Engineering and Technology (ICSET), pp. 148-152, 2011.

[28] Jayakumar.C and Chellappan.C, "Optimized on demand routing protocol of mobile adhoc network", Informatica, vol.17, no. 4, pp.481-502.

[29] Putri Ratna. A.A, Depok, Dewi Purnamasari.P, Shaugi.A, Salman.M "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system", in Proc. International Conference on QiR (Quality in Research), pp. 99-104, June 2013.

[30] Kumar.K.D, Ramya.I, Masillamani.M.R, "Queue Management in Mobile Adhoc Networks (Manets)" , IEEE/ACM Int'l Conference on Green Computing and Communications (GreenCom), & Cyber, Physical and Social Computing (CPSCom), pp.943-946, Dec. 2010.

[31] Ruoshan Kong, "The Simulation for Network Mobility based on NS2", in Proc. International Conference on Computer Science and Software Engineering, pp. 12-14,Apr'2008.

[32] Sachi Pandey and Vibhore Tyagi, "Performance Analysis of Wired and Wireless Network using NS2 Simulator", International Journal of Computer Applications, vol. 72, no. 21, pp. 38-44, Jun. 2013.

[33] Marko Korkalainen, Mikko Sallinen, Niilo Kärkkäinen, Pirkka Tukeva, "Survey of Wireless Sensor Networks Simulation Tools for Demanding Applications", in Proc. International Conference on Networking and Services ICNS, pp. 102-106, April 2009.

[34] Jun Zou, Dongmei Zhao, "G-BFS: A Scheme for Scheduling Real-Time CBR Traffic in IEEE 802.11-Based Mesh Networks", in Proc. IEEE Wireless Communications and Networking Conference, WCNC, pp.4268-4273, March, 2007.