Mobile Ad-Hoc Network Performance Measures Using NCTU Simulation

Hitesh Kumar[1], Dr. Rainu Nandal[2]
Scholar[1], Assistant professor[2]
University Institute of Engineering & Technology, MDU, Rohtak, India

Abstract
In Wireless sensor networks, Data Aggregation are dynamic methods to achieve latent control within the detecting group system. In several presentation such as: wireless sensing component network, data handling, and cloud processing, facts aggregation is commonly used. As the sensor knobs are battery determined, effective power consumption is essential to decrease the cooperated knobs and transportation thereby decreasing the facts sent to base station by increasing the network lifecycle. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks where, the structure of the network changes dynamically. A challenge to facts aggregation is thought to protect aggregative material from compromise node attacks and revealing during aggregating technique to obtain exact aggregative results. In this paper our chief focus is to study the mobile ad-hoc network environment and the performance measure on the basis of various parameter like packet dropped, throughput and packet collision.
Keywords: sensing knob, aggregation method, identification, compromise, network lifecycle.

INTRODUCTION

A wireless ad-hoc network is a collection of mobile nodes with no pre-established infrastructure or centralized administration. Wireless Sensor Networks is the grouping of sensor nodes, sensor nodes are used to sense the network by detecting events in the surrounding environment. It has two components i.e. aggregation points and base stations. Aggregation point gather the data about neighbour's sensors to aggregate them and pass the data to base terminal. Base station is also known as the gateway or access point [2]. WSN's schema consist of sensor nodes, network manager, security manager, aggregation points, base stations and user interface [4]. There can be application dependent additional components such as a location finding system, a Power generator and a mobilizer. Sensing unit consists of the sensor deployed at the node which collects data at the ground level. This data is the physical or the raw data which is sampled and converted to the analog domains and then into the digital form which is then converted into digital forms which is then sent to the processing unit. The processing unit mainly provides intelligence to the sensor node. The processing unit consists of a microprocessor, which is responsible for control of the sensors, execution of communication protocols and signal processing algorithms on the gathered sensor data. Transmission unit transfer data with the help of microcontrollers, transceivers and power units.

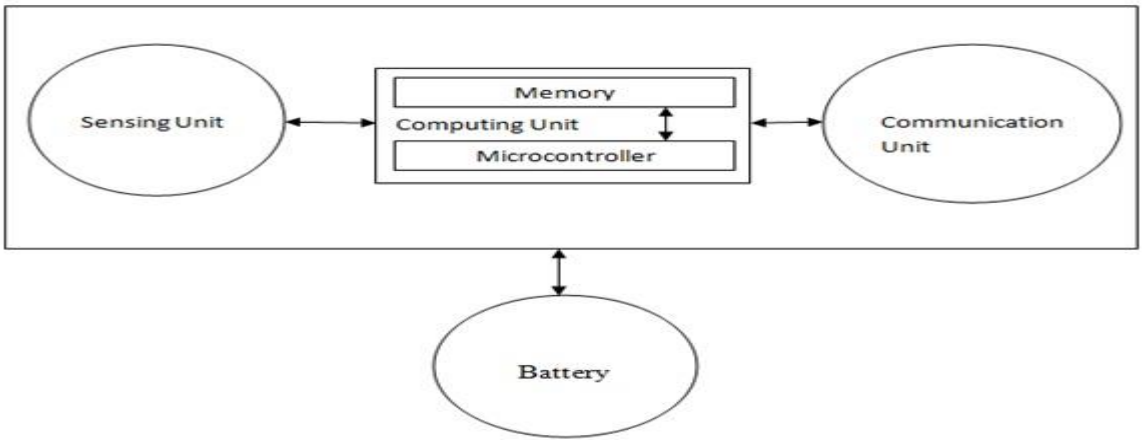

Figure 1.1 WSN Components

In wireless sensor network, data accuracy is essential; because these networks typically used on secured surroundings [12]. The central security key sockets on wireless sensor network, includes data (reliability, confidentiality), source (confirmation, approval) and system (reliability, availability).

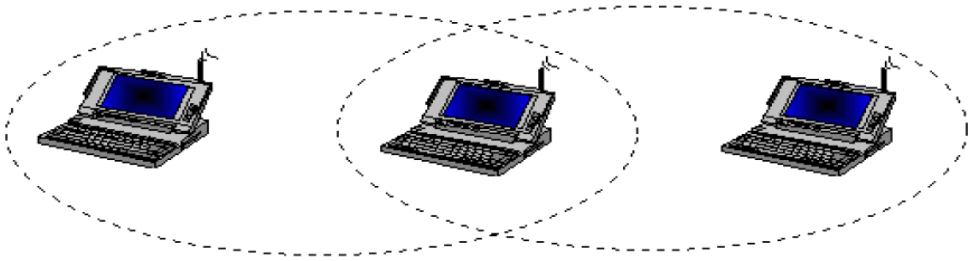

Figure – 1.2: Example of simple ad-hoc network

Figure-1.2 shows a simple ad-hoc network with three nodes. The outermost nodes are not within reception range of each other and thus cannot communicate directly. However, the middle node can be used to forward packets between the outermost nodes. This enables all three nodes to share information and results in an ad-hoc network.

Table I. Layer and Associated Threats [17]

Layers	**Threats**
Physical	Squeezing, Tempering
Data Link	Collision, Exhaustion, Unfairness
Network	Sinkhole, Wormhole, Selective Forwarding
Transport	Flooding, Synchronization problem
Application	Reliability Attack, Clock Skewing, Fact Aggregation, Distortion

Fact accumulation [18] is defined as the mechanism of collecting the data from diverse sensors to eliminate surplus transmission and deliver shared data to the base station.

Figure 1.3 Intrusion Detection Engine

Figure 1.3 represents the intrusion detection engine in wireless sensor network. Intrusion detection engine consist of a detection system, routing statistics, and alert system connected in block to identify the intrusion in the cluster of three wireless sensor node in which every group consist of one cluster head, one cluster member in a feed forward arrangement. Two cluster member are connected with the one cluster head to make a sensor network.

Literature Work

Several examiners have been employed on wireless sensor arena to deliver security mechanism to suits the resource guarded due to rising request of claims in penetrating areas. In [1] rule centred method is used to identify the sinkhole attack. They make dual rules and fixed in Intrusion detection scheme. When lone of the rule is disrupted by one of the nodes, the intrusion detection scheme activated an alarm but it does not deliver node unique identity of co-operated node. In [2] anomaly grounded identification scheme is used to detect the sink hole attack where the common consumer behavior is well-defined and intrusion identification is penetrating for something that is abnormal in the network. The received signal strength indicator valued is used with extra monitor node to identify the sink-hole attack in interconnected node. The other approach is statistical method identified by the researcher to detect the sink-hole attack in network. Statistical Girshick Rubin Shyriaev based algorithm is used to detect the malicious nodes in wireless sensor network [3]. Base station calculates the difference of CPU usage of each node after monitoring the CPU usage of each node in fixed time. Base station would identify whether a node is malicious or not after comparing the difference of

CPU usage with the threshold. Dynamic trust management system also used to detect and eliminate multiple attacks such as sinkhole attack. Each node calculates the trust of its neighbor node based on experience of interaction; recommendation and knowledge then sends to base station.

The routing mechanisms designed for wired networks are not adequate for ad-hoc networks due to their dynamic topology. To enable transmission between sender and receiver, the density of nodes should be high enough to provide connectivity [1]. Multi-hop routing protocols face the following two challenges. First, finding and choosing a path from the source node to the destination node, given no initial information, is complex and requires some form of global flooding of the network. Second, nodes in an ad-hoc network are mobile and communication is unstable.

PROTOCOLS

1. Reactive Routing Protocols

Reactive routing protocols, such as the Dynamic Source Routing (DSR) [3] and Ad-hoc On-demand Distance Vector (AODV) [4] routing protocols, are source initiated on demand routing protocols. This type of routing protocol creates routes only when requested by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network.

2. Proactive Routing Protocols

Proactive routing protocols, such as the Destination-Sequenced Distance-Vector (DSDV) [5], the Topology Broadcast Based on Reverse-Path Forwarding (TBRPF) [6] routing protocols, Optimized Link State Routing (OLSR) [7], and Open Shortest Path First with Minimum Connected Dominating Sets (OSPF-MCDS) [8], maintain up-to-date routing information using periodic control messages. Therefore, proactive routing protocols are ready to exchange packets at any time.

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it establishes a route on-demand when a transmitting mobile node requests one. Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad-hoc networks and other wireless ad-hoc networks. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand [21]. AODV is capable of both unicast and multicast routing [22]. DSDV is based on classical Bellman-Ford routing algorithm designed for MANETS. Each node maintains a list of all destinations and number of hops to each destination. Each entry is marked with a sequence number. It uses full dump or incremental update to reduce network traffic generated by rout updates. The broadcast of route updates is delayed by settling time. The only improvement made here is avoidance of routing loops in a mobile network of routers.

PERFORMANCE MEASURES

In this paper three performance measures are used which are as follows:

1. Packet Collision 2. Packet Drop 3. Throughput

When two or more stations attempt to transmit a packet across the network at the same time, a packet collision occurs. Packet drop occurs when one or more packets of data travelling across a computer network fail to reach their destination. Throughput is the average rate of successful message delivery over a communication channel.

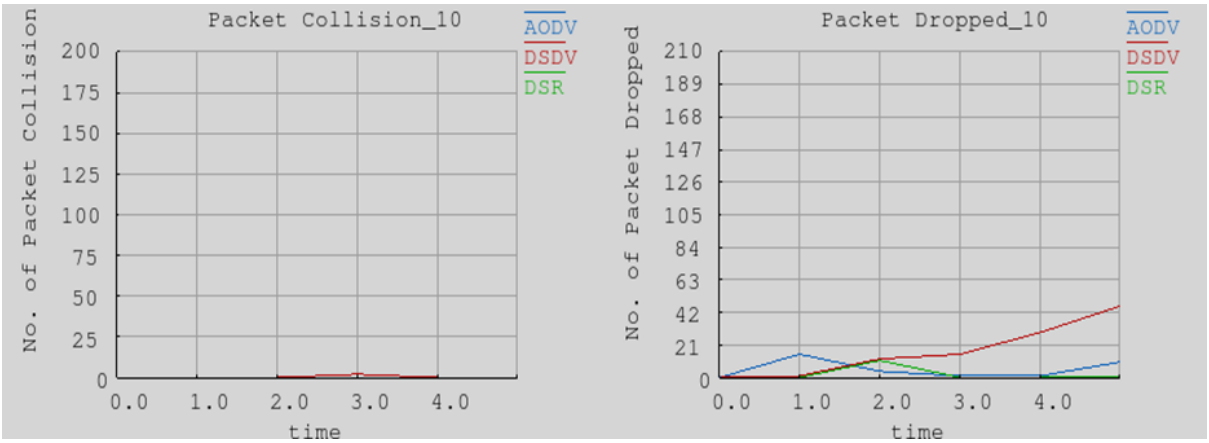

Figure 1.4 Execution Scenario of Packet Collision & Packet Dropped

In figure 1.4 graphs represents the result retrieved by setting up the mobile ad-hoc network with ten nodes. In first graph it represents the packet collision output executing in NCTU simulator. In second right part of the

graph represent the packet dropped execution scenario in simulator with ten nodes. In this work we have used three protocols for performance measure via different parameters.

Table II Simulation Parameters for NCTU

Parameter	Value
Simulation time	180 Sec.
PHY-MODEL	802.11 b
Number of Nodes	10,30,60
Node Movement	Random
Channel Frequency	2.4 GHz

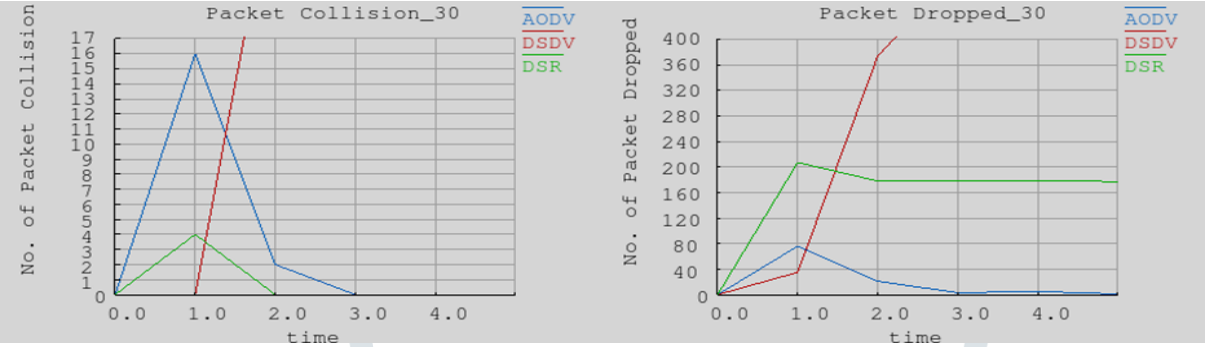

Figure 1.5 Execution Scenario of Packet Collision & Packet Dropped with 30 nodes

In terms of Packet collision DSR performs well as compared to DSDV and AODV, when the number of nodes is less as the load will be less. However the number of packet collision decreases when we increase the nodes. The number of packet collision increases in DSDV when we increase the number of nodes. As the graph shows that the no. of packet collisions in DSDV is very high as compared to AODV and DSR. So we can say that the performance of DSDV is worst among all the three protocols. The performance of AODV is initially very high but consistent as the number of packet increases. So from the graph it is clear that the overall performance of DSR is better.

In terms of packets dropped DSDV's performance is the worst as compared to AODV and DSR. The performance degrades with the increase in the number of nodes. The performance of AODV is better than the DSDV and DSR when the number of nodes are less but decreases when we increase the number of nodes. DSR performs consistently well with increase in the number of nodes.

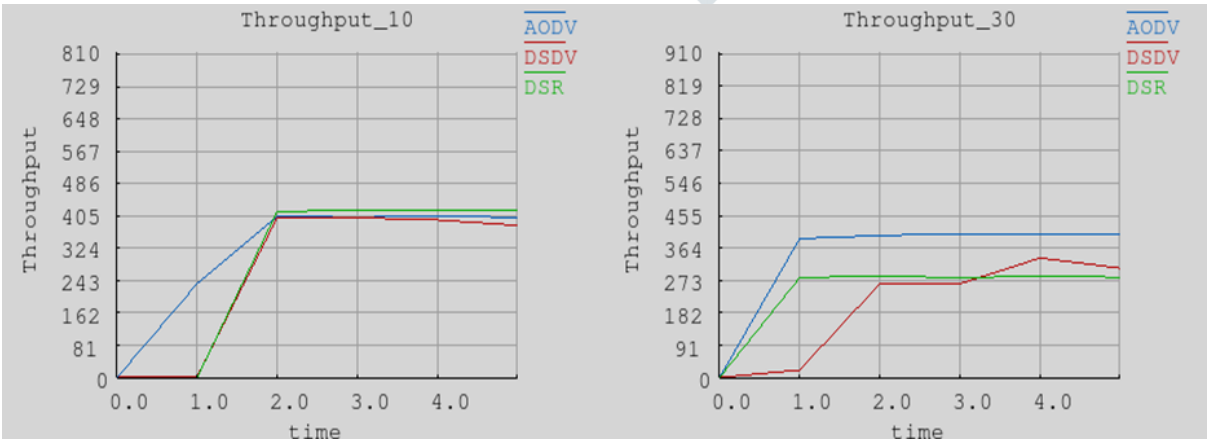

Figure 1.5 Execution Scenario of Throughput

In terms of throughput the performance of DSR and AODV are almost uniform and better than the DSDV. The performance of DSDV is degrading due to increase in the number of nodes the load of exchange of routing

tables becomes high and the frequency of exchange also increases due to the mobility of nodes. So from the graph it is clear that the performance of DSDV is worst.

Conclusion

Our results indicate that the performance of the two on demand protocols namely DSR and AODV is superior to the table driven DSDV in conformance with the work done by other researchers. It is also observed that DSR outperforms AODV in less stressful situations, i.e. smaller number of nodes. As far as packet collision and packets dropped ratio are concerned, DSR and AODV performs better than DSDV with large number of nodes. Hence for real time traffic AODV is preferred over DSR and DSDV. For less number of nodes and less mobility, DSDV's performance is superior. A general observation is that protocol performance is linked closely to the type of MAC protocol used. For example, if MAC protocol sends packets in bursts, it is observed that many route error packets are being sent in response to bursts of packets moving on invalid paths. In conclusion, the design of the routing protocol must take into consideration the features of the lower layer protocols.

Refrences

[1] Krontiris, Ioannis & Giannetsos, Thanassis & Dimitriou, Tassos. (2008). LIDeA: A distributed lightweight intrusion detection architecture for sensor networks. Proceedings of the 4th international conference on Security and privacy in communication netowrks - SecureComm '08.

[2] P. Johansson, T.Larsson, N.Hedman, B.Mielczarek, M.Degermark, Scenariobased Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks, Mobicom _99 Scattlc Washington USA, pp. 195-206

[3] L. Lazos and R. Poovendran, "Serloc: Robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 1, pp. 73–100, 2005.

[4] T. Dimitriou and I. Krontiris, *Security in Sensor Networks*. CRC Press, 2006, ch. Secure In-network processing in Sensor Networks, pp. 275– 290.

[5] S. Ganeriwal, S. Capkun, C.-C. Han, and M. Srivastava, "Secure time synchronization service for sensor networks," in *Proceedings of the 4th ACM workshop on Wireless security (WiSe '05)*, 2005, pp. 97–106.

[6] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05)*. ACM Press, October 2005, pp. 16–23.

[7] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, vol. 3, Montreal, Canada, August 2005, pp. 253–259.

[8] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, 2005.

[9] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006.

[10] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48–60, February 2004.

[11] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Realworld physical attacks on wireless sensor networks," *Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC)*, pp. 104–118, April 2006.

[12] C.E. Perkins and E.M. Royer, Ad hoc On Demand Distance Vector Routing, University of California, Santa Barbara.

[13] O. Kachirski, R. Guha, D. Schwartz, S. Stoecklin, and E. Yilmaz, "Casebased agents for packet-level intrusion detection in ad hoc networks," in *Proceedings of the 17th International Symposium on Computer and Information Sciences*. CRC Press, October 2002, pp. 315–320.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MobiCom '00)*, 2000, pp. 255–265.

[15] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Department of Computer Engineering, Chalmers University of Technology, Tech. Rep. 99-15, March 2000.

[16] Z. Benenson, F. C. Freiling, B. Pfitzmann, C. Rohner, and M. Waidner, "Verifiable agreement: Limits of non-repudiation in mobile peer-to-peer ad hoc networks," in *Third European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Hamburg, Germany, Sept. 2006.

[17] S.Ranjeeth Kumar, "SSLEACH: Specification based Secure LEACH Protocol for Wireless Sensor Networks", 978-1-4673-9338-6/16/$31.00_c 2016 IEEE.
[18] Krithika S, "Enhanced Data Aggregation Techniques for Compromised Node Attacks in Wireless Sensor Networks", presented at the IEEE WiSPNET 2016 conference, 978-1-4673-9338-6/16/$31.00_c 2016 IEEE.
[19] Krontiris Ioannis¤, Tassos Dimitriou¤and Felix C. Freiling (2007), "Towards Intrusion Detection in Wireless Sensor Networks", Proceedings of the 5th international conference on Security and privacy in communication netowrks - SecureComm '07
[20] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *AdHoc Networks Journal*, vol. 1, no. 2–3, pp. 293–315, September 2003.
[21] C.E Perkins, E.M. Royer, and S. Das, Ad hoc On-demand Distance Vector (AODV), RFC 3561, July 2005.

[22] C.E. Perkins and E.M. Royer, Ad-hoc On-Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999.