International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 4 July-August 2017 p-ISSN: 2394-8280

HLA BASED SOLUTION FOR PACKET LOSS DETECTION IN MOBILE AD HOC NETWORKS

Dr. Shoban Babu[1],Prof. Mangesh Ingle[2],Prof. Ashish Mahalle[3]
[1]Associate Professor , Department of Computer Engineering,
Varadha Reddy College of Engineering, SR Group of Colleges
[2,3]JCOET, Yavatmal
babuack@yahoo.com

ABSTRACT

Packet drooping is one of the concerns in wireless networks. It is there in Mobile Ad Hoc Networks (MANETs) as well. MANET is the network which is established when situation demands for effective communications. Nodes in the network act as both sender and receiver of data packets. When data packets are reaching destination as sent by the sender, it is perfectly ok. However, it is seen generally some packets are lost while transmitting data. Data loss can occur due to either bad channel conditions or malicious attacks. Finding the reason behind packet loss besides detecting packet loss is very important in mobile networks. In this paper, we proposed and implemented a solution for this problem. Our solution is based on Homomorphic Linear Authenticator (HLA). It is used to detect packet loss and find the reason for it. The solution is implemented with a custom simulator build in Java programming language. The results showed the utility of the proposed approach.

Index Terms – Wireless Ad Hoc Network, packet dropping, auditing

INTRODUCTION

In networks with multiple hops, there is cooperation between nodes in order to send packets from source to destination. It does mean that the packets cannot be sent from source to destination directly without the active cooperation of intermediate nodes. In this context, it is possible that certain nodes misbehave and just drop packets without forwarding to neighbour nodes. This is the potential problem in wireless ad hoc networks. Packets are the important things in network traffic that carry actual data. When packets are lost, the data is lost. Thus quality of communication gets deteriorated and the quality of content is reduced. In case of high priority delay insensitive traffic such as live cricket match, it is essential to ensure that packets are not dropping. When packets are dropped for any reason, the quality of rendered video is reduced. This is the potential risk with respect to content dissemination. This needs to be prevented by devising mechanisms that can handle packet dropping.

As a matter of fact, packet dropping can be done due to reasons such as link errors and malicious attacks. The former is due to natural problems in the wireless channels while the latter is manmade. Some insider attacks in this paper are expected to participate or cause damage to traffic by dropping packets intentionally. The existing applications either focused on packet dropping caused by link errors or attacks. Many existing mechanisms simply consider packet dropping due to attacks. They do not differentiate packet loss due to link error and packet loss due to an attack. In this paper we proposed a public auditing based solution which demonstrates the proof of concept. The system is implemented in the form of a custom simulator developed using Java platform. The empirical results revealed that the proposed system is able to differentiate between packet losses due to link error from that caused by malicious attacks. The remainder of the paper is structured as follows. Section II provides review of literature. Section III presents the proposed system in detail. Section IV presents experimental results while section V concludes the paper.

RELATED WORKS

Malicious packet drops and packet drops due to link errors is the differentiation shown by detection algorithms generally. High malicious dropping rates and low link errors in one pattern. The second pattern is high link errors and low packet dropping rates. Literature found on this is divided into

e-ISSN: 2394-8299
p-ISSN: 2394-8280

different categories base on approach used to identify attacking nodes. The categories are known as credit systems, reputation based systems, end-to-end acknowledgements, and cryptographic methods. The first category is credit systems that are based on the incentives given to nodes when they behave well. Thus it motivates nodes to be genuine. These solutions are explored in [1], [2] and [3]. The second category is reputation based. It is based on monitoring of nodes that misbehave. This reputation system gives good reputation or bad reputation to neighboring nodes. Based on the reputation of nodes, they are trusted. Reputation of nodes is used for making important decisions like root selection. This category of research is found in [4], [5], [6], [7], [8], [9], and [10].
The third category is based on the hop-to-hop and end-to-end acknowledgements with respect to losing packets. When any node is found with high packet loss rate, it is excluded from the network and it is eliminated while making route section as well. This kind of research is found in [11], [12], [13], [14], [15], and [16]. The fourth category is based on cryptographic primitives. These primitives as explored in [17], [18] and [19] are widely used to have secure communications in WSN. Especially they focused on packet dropping. They used techniques like Bloom Filters identification of suspicious loops, tracing forwarding records and so on. Modeling traffic at MAC layer is explored in [20] for examining packet drops. All intermediate nodes are able to envisage packet dynamics and find discrepancy in rates of packets in order to differentiate malicious dropping from other means of packet dropping. In this paper, we simulate WSN environment and demonstrate packet dropping detection using a public auditing approach. The proposed system is actually a custom simulator built using Java programming language.

PROPOSED SYSTEM

We proposed public auditing based packet drop detection mechanism. The architecture of the proposed system is shown in Figure 1. The network involves service provider or sender, receiver and router. It is to simulate the multihop environment with intermediate nodes cooperating for packet forwarding. An attacker module is implemented in order to demonstrate packet dropping and its detection.

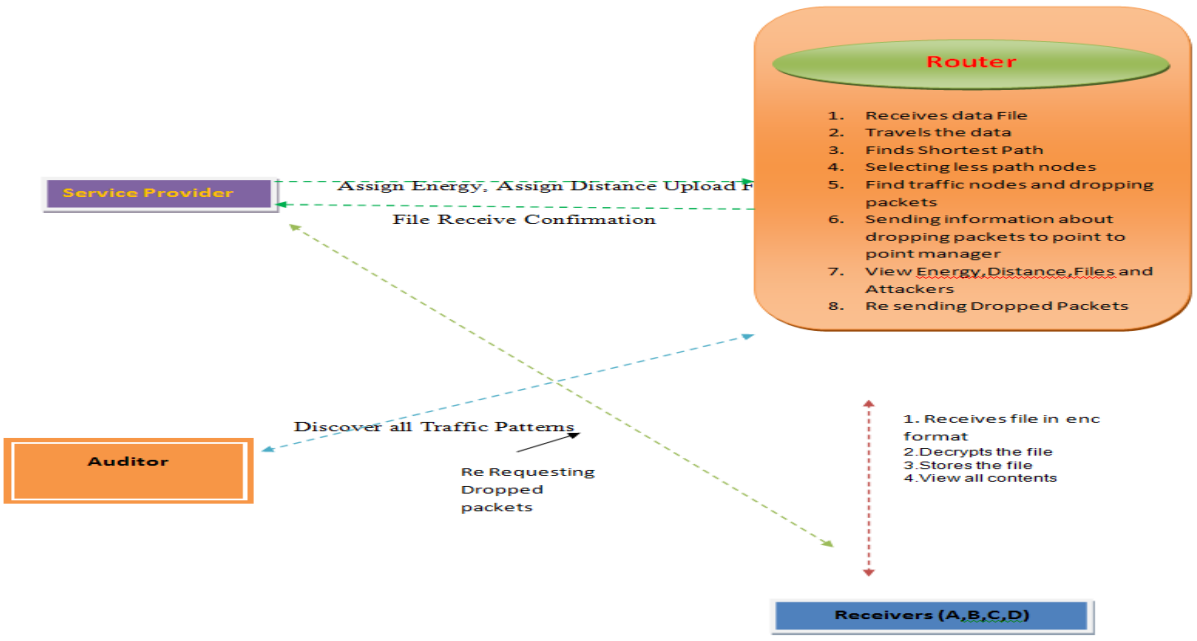


Figure 1 – Proposed architecture for simulation

As shown in Figure 1, the service provider acts as sender of information. The receiver acts as destination. The router is the intermediate node which is meant for forwarding packets to destination

e-ISSN: 2394-8299
p-ISSN: 2394-8280

node. The auditor actually performs the detection logic in order to know whether packets are dropped due to link failure or malicious attack on the node.

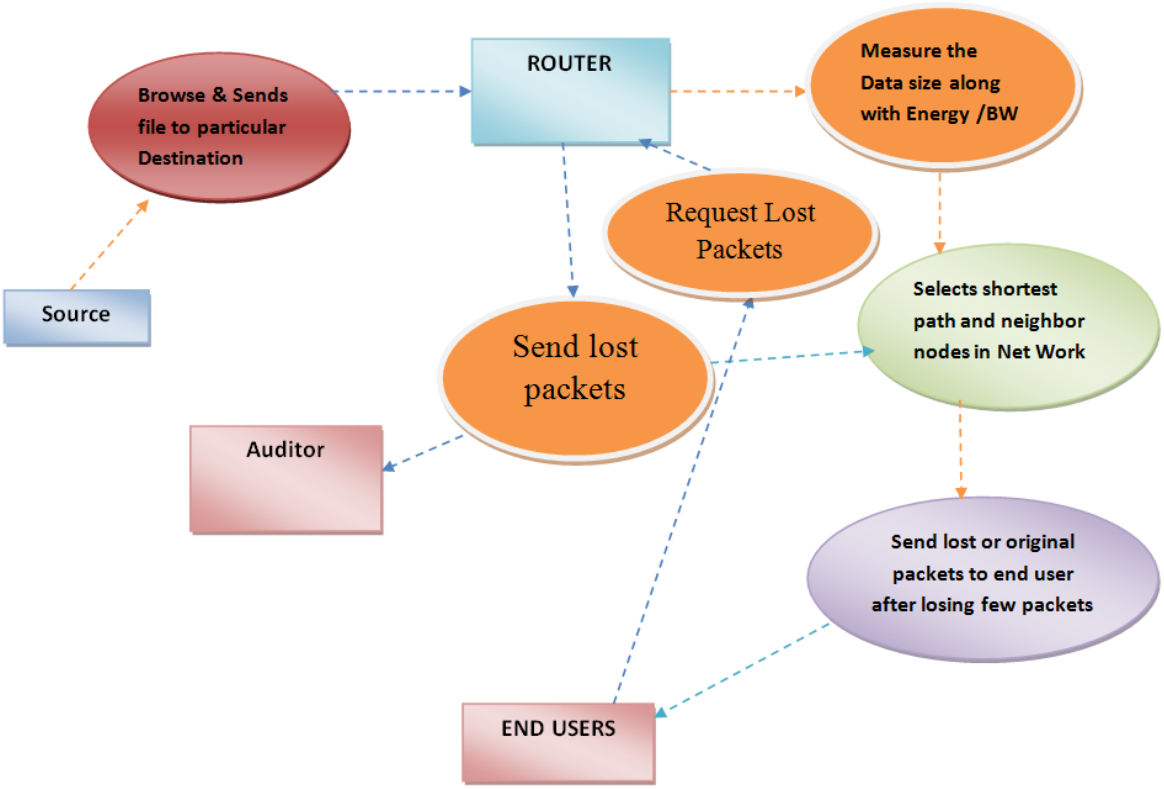


Figure 2 – Shows the flow of information

As shown in Figure 2, it is evident that there is information flow in the system. The source node sends data to destination through router. However, the router performs operations such as measuring data size, bandwidth and energy, request lost packets and sending packets. The auditor is involved in monitoring tartaric for taking well informed decisions. The end users are nothing but destination where information reaches.

IMPLEMENTATION AND RESULTS

We implemented a wireless network simulator using Java platform to demonstrate the proof of concept. The functionalities of the proposed system are divided into multiple modules namely service provider, router, auditor, destination and attacker. The modules are described here. They are implemented using Java swing API, I/O and networking API. The implementation is a networking application that encapsulates sender, receiver and router functionalities.

Service Provider

In this module, the service provider browses the file and sends to the particular end users via router. And also service provider can assign energy and assign distances for the nodes in router.

Router

In this module, the router sends the file from source to destination (from service provider to end users) by selecting shortest distances between two nodes & sufficient node energy. And if node has less energy than file size then packet dropper in router drops the some packets from file and sends remaining file to the destination. And it can also do some operations like view distances, view energy, view files, view attackers, verify, refresh.

Auditor

In this module, the auditor discovers the traffic pattern, means it stores the details of dropped packets. It contains details of in which node packets are dropped, how many no of packets dropped, from which file dropped & status of packets.

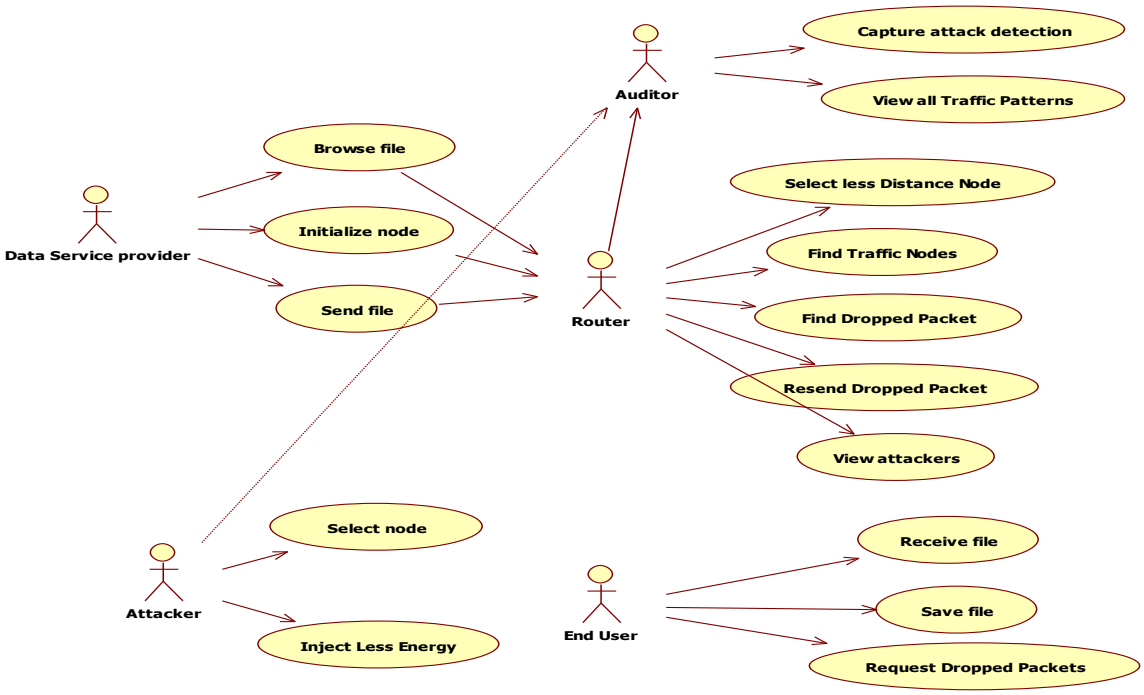
Destination (End User)

In this module, there are n no of destinations (A, B, C….). These end users only receive the file from service provider via router. While getting the file from service provider there may be chances of packets dropping, if packets are dropped then end user will gets dropped packets from point to point manager. The end users receive the file by without changing the File Contents. Users may receive particular data files within the network only.

Attacker

Attacker is one who makes changes the energy of particular nodes in router. And all attackers' details stored in router with their all details such as attacker Ip address, attacked node, modified energy and attacked time.

The use cases in the proposed system include browse file, initialize node, send file, select node, inject less energy, capture attack detection, view all traffic patterns, select less distance node, find traffic nodes, find drop packets, resend dropped packets, view attackers, receive file, save file and request dropped packets. These use cases are associated with different actors shown in Figure 2.



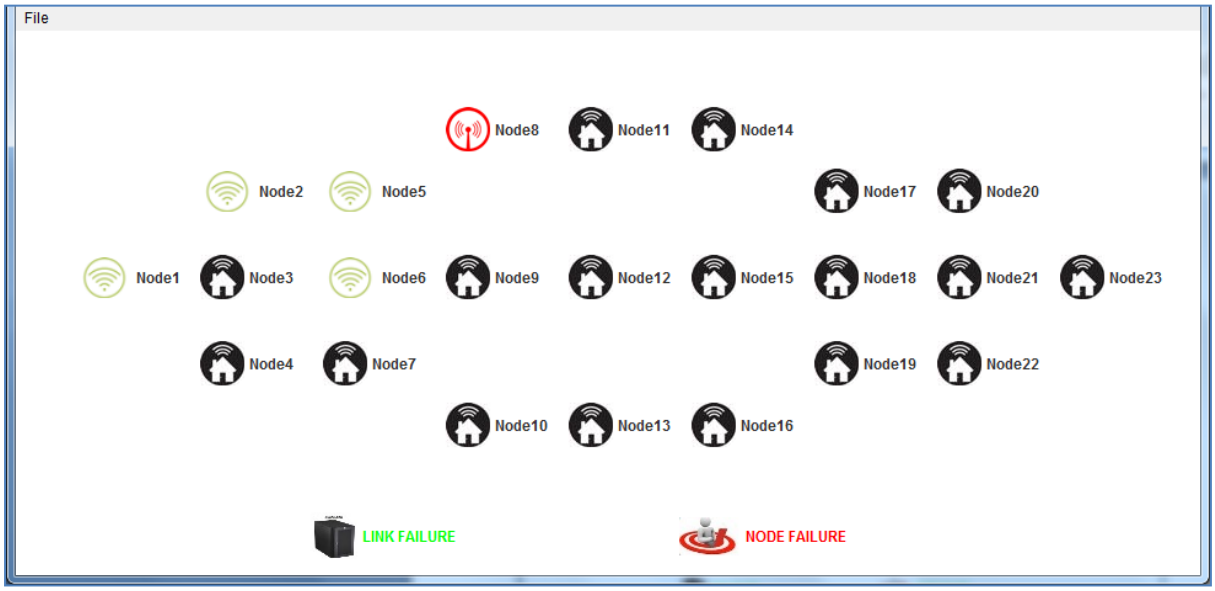
e-ISSN: 2394-8299
p-ISSN: 2394-8280

Figure 2 – Use case of the proposed solution

As shown in Figure 2, it is evident that the use cases are associated with different actors in order to have modular functionality to simulate detection of packet drop in wireless ad hoc networks. The simulation demonstrates nodes as windows and there is communication among them. The attack scenario is considered to demonstrate the purpose of the proposed system.

Figure 3 – Multiple nodes are involved in the simulation

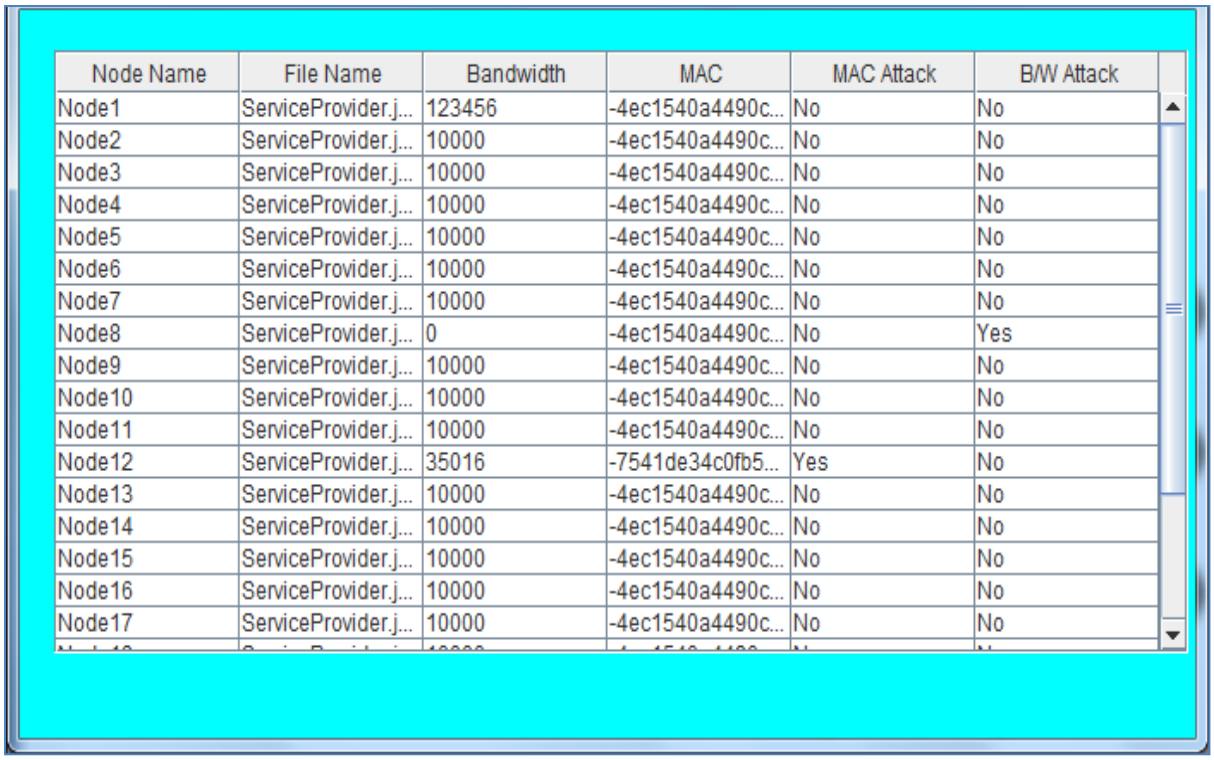
As shown in Figure 3, the router side visualization is presented. There are many nodes involved in the network. Based on the proposed implementation the nodes are simulated. The simulation also provides details of packet dropping and identification of nodes are prone to involve in packet dropping attacks. The simulation also demonstrates the differentiation of packet dropping due to link error from that of malicious attacks.



e-ISSN: 2394-8299
p-ISSN: 2394-8280

Figure 4 – Shows Node 8 differently in the simulation

As shown in Figure 4, it is evident that node 8 is compromised and that is causing packet dropping attack.



Node Name	File Name	Bandwidth	MAC	MAC Attack	B/W Attack
Node1	ServiceProvider.j...	123456	-4ec1540a4490c...	No	No
Node2	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node3	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node4	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node5	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node6	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node7	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node8	ServiceProvider.j...	0	-4ec1540a4490c...	No	Yes
Node9	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node10	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node11	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node12	ServiceProvider.j...	35016	-7541de34c0fb5...	Yes	No
Node13	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node14	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node15	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node16	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No
Node17	ServiceProvider.j...	10000	-4ec1540a4490c...	No	No

Figure 5 – Showing the simulation results

As shown in Figure 5, the complete simulation is shown with verbose output. The results revealed the probability of attacks.

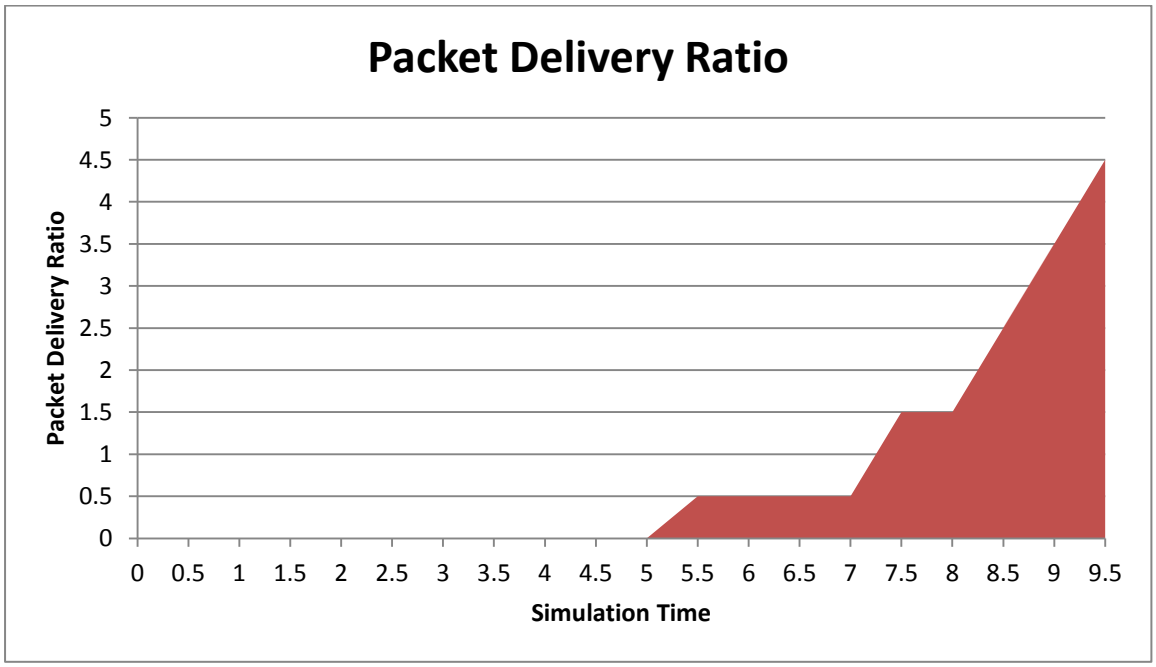


Figure 4 – Packet Delivery Ratio

e-ISSN: 2394-8299
p-ISSN: 2394-8280

As shown in Figure 4, the simulation time and packet delivery ratio are represented by horizontal and vertical axes respectively. The results revealed that as simulation time increases the packet delivery ratio is increased.

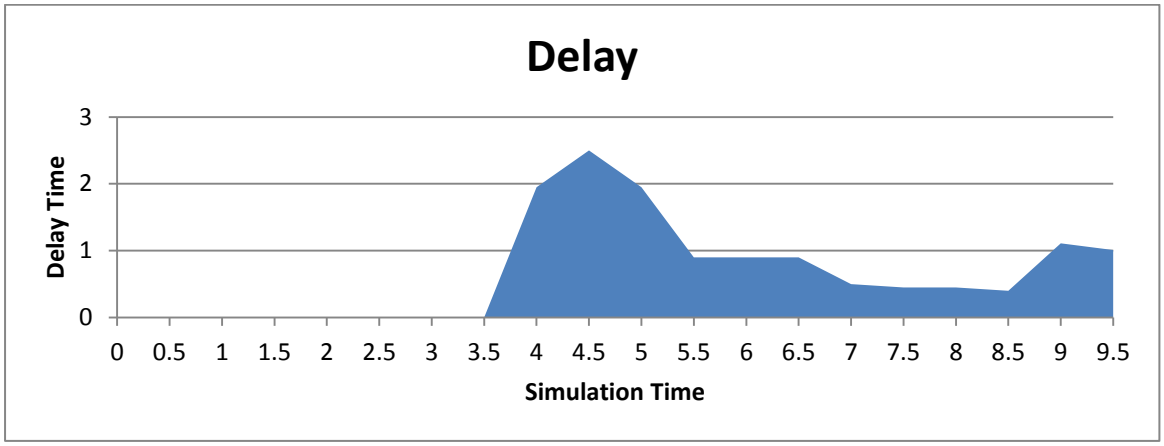


Figure 5 – Delay performance

As shown in Figure 5, the simulation time and delay time are represented by horizontal and vertical axes respectively. The results revealed that as simulation time increases the delay is increased. But it is more in the middle of simulation.

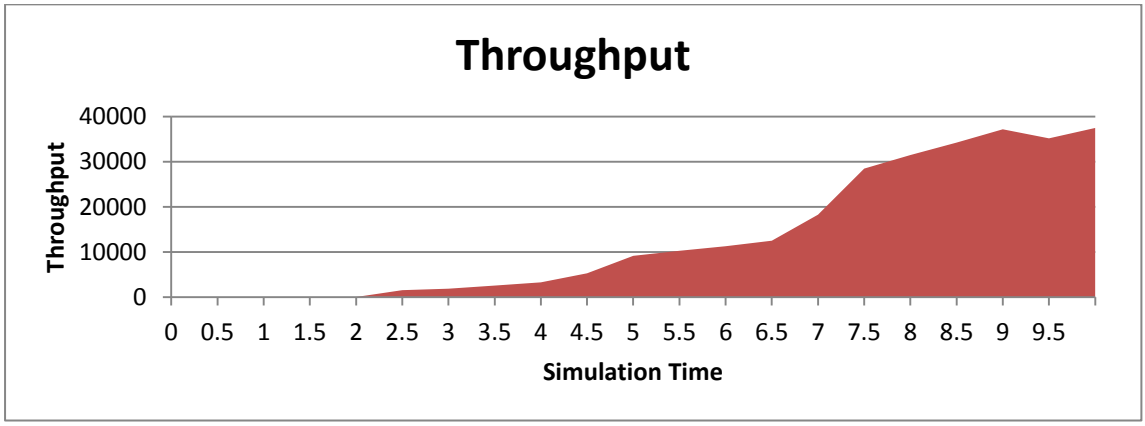


Figure 6 – Throughput

As shown in Figure 6, the simulation time and throughput are represented by horizontal and vertical axes respectively. The results revealed that as simulation time increases the throughput ratio is increased.

e-ISSN: 2394-8299
p-ISSN: 2394-8280

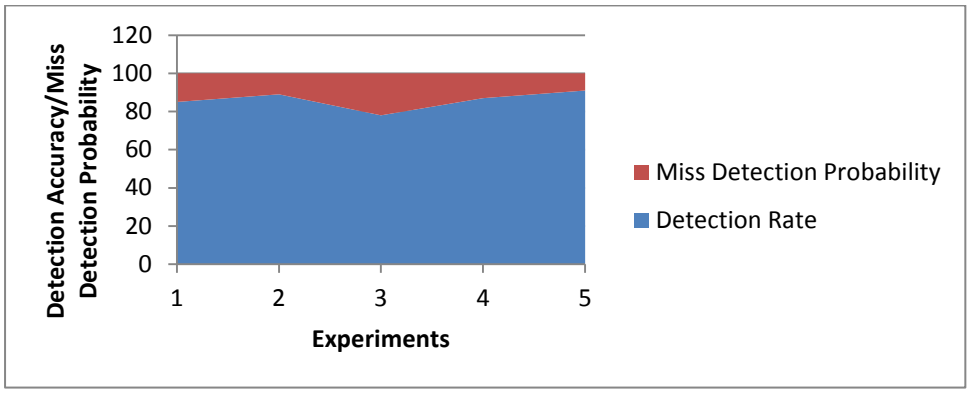


Figure 7 – Packet drop detection accuracy

As shown in Figure 7, it is evident that five experiments and their results are presented in terms of detection rate and miss detection probability.

CONCLUSIONS AND FUTURE WORK

In this paper, we studied the packet dropping problem in MANET. Packet dropping causes deterioration of quality of data transmission. Especially, in case of video data, it causes the problem to the viewers of videos. In the literature it is found that packet loss is due to either link failures or attacks. However, most of the solutions were based on the assumption that packet loss is due to attacks only. In this paper we proposed a method based on HLA in order to detect packet loss and find the exact reason for it. The method truthfully examines the reason for the packet drop is either link failure or malicious attacks. Simulation study is made in order to have proof of the concept. The results revealed that the proposed method is effecting in finding or detecting packet loss in MANET. In also helped in finding the actual cause of the packet drop. In future, we intend to find the dynamics of packet loss with more focused research in different kinds of networks.

REFERENCES

[1] J. N. Arauz, “802.11 Markov channel modeling,” Ph.D. dissertation,School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.
[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable data possession at untrustedstores,” in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007,pp. 598–610.
[3] G. Ateniese, S. Kamara, and J. Katz, “Proofs of storage from homomorphicidentification protocols,” in Proc. Int. Conf. Theory Appl.Cryptol. Inf. Security, 2009, pp. 319–333.
[4] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, “Castor: Scalable secure routing for ad hoc networks,” in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.
[5] S. Buchegger and J. Y. L. Boudec, “Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhocnetworks),” in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.
[6] Q. He, D. Wu, and P. Khosla, “Sori: A secure and objective reputation- based incentive scheme for ad hoc networks,” in Proc. IEEEWireless Commun. Netw. Conf., 2004, pp. 825–830.
[7] Y. Liu and Y. R. Yang, “Reputation propagation and agreement in mobile ad-hoc networks,” in Proc. IEEE WCNC Conf., 2003,pp. 1510–1515.
[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks,” in Proc. ACM MobiComConf., 2000, pp. 255–265.
[9] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, “Routing amid colluding attackers,” in Proc. IEEE Int. Conf. Netw. Protocols, 2007,pp. 184–193.
[10] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H.Rubens, “ODSBR: An on-demand secure byzantine resilient routingprotocol for wireless ad hoc networks,” ACM Trans. Inform. Syst.

Security, vol. 10, no. 4, pp. 1–35, 2008.
[11] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, “An acknowledgement- based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.
[12] V. N. Padmanabhan and D. R. Simon, “Secure traceroute to detect faulty or malicious routing,” in Proc. ACM SIGCOMM Conf., 2003, pp. 77–82.
[13] P. Papadimitratos and Z. Haas, “Secure message transmission in mobile ad hoc networks,” Ad Hoc Netw., vol. 1, no. 1, pp. 193–209, 2003.
[14] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, “ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks,” ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.
[15] Sriramoju Ajay, B. (2017). INTELLIGENT MOBILE APP FOR FINDING PATH AND TRACKING POST PACKETS USING ANDROID PLATFORM. International Journal Of Research In Science & Engineering, 3(2), 9.
[16] Sriramoju Ajay, B. (2017). Investigation of Feasible Tourist Destinations using Android Mobile App. International Journal Of Research In Science & Engineering, 3(2), 9.
[17] Babu, Sriramoju Ajay, and Namavaram Vijay. "Image Tag Ranking for Efficient Matching and Retrieval." (2016).
[18] Babu, Sriramoju Ajay, and Namavaram Vijay. "Design and Implementation of a Framework for Image Search Reranking." (2016).
[19] Babu, Sriramoju Ajay and Babu, S Shoban. "International Journal of Research and Applications Jan-Mar© 2016 Transactions 3 (9): 422-426 eISSN: 2349–0020."
[20] Babu, Sriramoju Ajay. "PARTICLE SWARM OPTIMIZATION ALGORITHM FOR ROUTING NETWORK" (2017).
[21] Babu, Sriramoju Ajay. "MODIFICATION AFFINE CIPHERS ALGORITHM FOR CRYPTOGRAPHY PASSWORD" (2017).
[22] Babu, Sriramoju Ajay. "Perceptual-Based Quality Metrics For Image and Video Services" (2015).
[23] Sriramoju, Ajay Babu. "Analysis on Image Compression Using Bit-Plane Separation Method" (2014).
[24] Babu, Sriramoju Ajay. "Objective Quality Metric Design For Wireless Image and Video Communication" (2014).
[25] Ajay Babu Sriramoju, Dr. S. Shoban Babu. "Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays For Image Processing" (2013).
[26] Sriramoju, Ajay Babu. "Image Processing: Lossy Compression by Color Quantization and Gct Modeling" (2012).
[27] Sriramoju, Ajay Babu. "Analysis on Lossless Image Compression in Image Processing" (2011).
[28] K. Balakrishnan, J. Deng, and P. K. Varshney, “TWOACK: Preventing selfishness in mobile ad hoc networks,” in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.
[29] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad-hoc routing service in adversarial environments,” Wireless Pers. Commun., Special Issue Secur. Next Generation Commun., vol. 29, no. 3, pp. 367– 388, 2004.
[30] W. Kozma Jr., and L. Lazos, “REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.
[31] W. Kozma Jr. and L. Lazos, “Dealing with liars: Misbehavior identification via Renyi-Ulam games,” presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009
[32] Y. Zhang, L. Lazos, and W. Kozma, “AMD: Audit-based misbehavior detection in wireless ad hoc networks,” IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.
[33] R. Rao and G. Kesidis, “Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited,” in Proc. IEEE GLOBECOM Conf., 2003, pp. 2957–2961.