International Journal of Academic Research and Development
ISSN: 2455-4197, Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 4; July 2017; Page No. 479-485

Availability & security of routing in wireless network

Meenu Kamboj

Department of Computer Science, UCKUK, Haryana, India

Abstract
Security is an essential service for wired and wireless network communications. It is very challenging for researchers to provide comprehensive security for wireless networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper, we review different protocols with a particular focus on security aspects. Secure wireless networks have to meet five security requirements: confidentiality, integrity, authentication, non-repudiation and availability. The analyses of the secure versions of the proposed protocols are discussed with respect to the availability and security of routing in wireless network. In the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In this paper, we examine routing attacks, such as link spoofing and colluding miserly attacks, as well as countermeasures against such attacks in existing MANET protocols. The proposed Scheme will take care to evaluate various security designs and to implement in existing protocols. Efforts will be made to make wireless networks data transfer reliable. Algorithm will be developed to achieve stable data transfer. Finally effort will be made to merge the existing scheme with new scheme to get better scalable design.

Keywords: wireless network, security, routing, stability

1. Introduction
A Wireless network is an emerging technology that has been attracting tremendous attention from researchers. Because these networks can be deployed quickly without relying on a predefined infrastructure, they can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces.

A Wireless network is a continuously self - configuring, infrastructure - less network of mobile devices connected without wires. Each device in a WIRELESS NETWORK is free to move independently in any direction, and will therefore change its links to other devices frequently. The main challenge in building a WIRELESS NETWORK is maintaining each device to continuously maintain the information required for proper routing of traffic. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

The backbone of the wireless network is routing. Routing is the process of forwarding packets from source to destination using most efficient route. Efficiency of the path/route is measured in various metric like number of hops, traffic, security etc. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency. All WIRELESS NETWORK routing protocols could be broadly classified into three major categories: Pro-active Routing Protocols, Reactive Routing Protocols, and Pro-active Routing Protocols.

2. Literature Survey
A WIRELESS NETWORK is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, WIRELESS NETWORK attracts different real world application areas where the networks topology changes very quickly [7].

However, in [8, 9] many researchers are trying to remove main weaknesses of WIRELESS NETWORK such as limited bandwidth, battery power, computational power, and security. Although a lot of work under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wired networks cannot be applied directly to WIRELESS NETWORK, which makes a WIRELESS NETWORK much more vulnerable to security attacks.

Some solutions in [8, 9, 10] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. Many researchers have developed lots of routing protocols in WIRELESS NETWORK. The on-demand routing is that set up a route to a target node whenever required in place of static route path. Almost every on-demand routing protocols reestablish a fresh route subsequent to a route break.

Dahill *et al.* proposed ARAN [11], it assumes managed-open environment, where there is a possibility for predeployment of infrastructure. It is prone to reply attacks using error messages unless the nodes have time synchronization.

Papadimitratos and Haas [12] proposed a protocol SRP that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected and any malicious node can just forge error messages with other nodes as source.

ARIADNE [13], is based on DSR [14] and TESLA [15]. It prevents attackers/compromised nodes from disrupting uncompromised routes comprising of benign nodes. It uses highly efficient symmetric key cryptography. It does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. It is vulnerable to active-1-1 attacker that lies along the discovered route, who does not forward packets and does not generate ERROR if it encounters a broken link. It also requires clock synchronization, which is considered to be an unrealistic requirement for wireless networks.

Perlman proposed a link state routing protocol [16] that achieves Byzantine Robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption.

Zhou and Haas [17] primarily discussed key management. They devote a section to secure routing, but essentially conclude that ―nodes can protect routing information in the same way they protect data traffic‖. They also observe that denial of- service attacks against routing will be treated as damage and routed around.

Some work has been done to secure wireless moving networks by using misbehavior detection schemes [18]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second has no real means to guarantee the integrity and authentication of the routing messages. Looking at the work that has been done in this area previously, it seems that the security needs for wireless networks has not been yet satisfied. Most of the work done around using Hashing techniques is around authenticating messages and route table entries.

Bayya *et al* [19] demonstrate the use of hashing as part of password based authenticated key exchange. The problems in this protocol are the need of a strong shared secret and the need to constantly change the shared secret which in turn may prove to be computationally expensive.

K. Lakshmi *et al*. analyzed and improved the security of one of the popular routing protocol. This work focused specifically, is on ensuring the security against the Black hole Attack. The proposed solution is that capable of detecting and removing black hole nodes in the WIRELESS NETWORK at the initial stage itself without any delay [20].

S. Taneja [21], proposes a new protocol SSRP (Stable and Secured Routing Protocol). Due to unbalanced node usage, some of the battery powered nodes drain out faster than others. This leads to route re-discovery causing larger average end to end delay and more control overhead. So scheme will be proposed to speed up the process.

3. Research Problem

- In Wireless Network it is hard for a route to sustain for a longer period of time due to the mobility of nodes. High mobility of nodes results in active route failure and re-route discoveries. Such frequent route discoveries result in decreased network performance. Therefore, the scheme will be proposed to make to increase network performance and data transfer reliable.
- Due to unbalanced node usage, some of the battery powered nodes drain out faster than others. This leads to route re-discovery causing larger average end to end delay and more control overhead. So scheme will be proposed to speed up the process.
- Wireless Network is ideally to be used in emergency situations like natural disasters, military conflicts, emergency medical situations etc. Therefore, this research will focus on proposing scheme.

4. Simulation and Analysis Method

Till now, comparative analysis have been done between two routing protocols naming AODV and DSR based on 3 parameter metrics Packet delivery Ratio, Average End-to-End delay and Throughput. The performance evaluation has been done using Network Simulator (NS2). The new scheme will be compared with existing schemes and performance evaluation will be done using graphs and their interpretations. Network simulator-2 is popularly used for ad-hoc networking community. It is the open source software for evaluating the performance of the existing network protocols and evaluates new network protocols before use. Using ns2 simulator to simulate a variety of IP networks.

The Routing protocols were compared based on 3 parameter metrics given below.

Packet delivery Ratio: Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic destination. It measures the loss rate as seen by transport protocols and as specific to both the correctness and efficiency of ad hoc routing protocols. A great packet delivery ratio is desired in any network.

Average End-to-End delay: The packet End-to-End delay is the average time that a packet takes to travel the network. This is the time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. Therefore includes all the delays in the network such as transmission times, buffer queues and delays induced by routing activities and MAC control exchanges.

Throughput: Throughput defined as the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

5. Results

Metrics have been used as the Packet Delivery Ratio for two protocols AODV and DSR. The simulations have been performed using Network Simulator 2 (NS-2.34) particularly popular in the ad hoc networking community. The traffic sources are TCP. The source-destination pairs are spread randomly over the network. During the simulation, each node starts its journey from a random spot to a random chosen destination. Different network scenario for different number of nodes and pause times are generated.

Output after applying this scale for varying pause time and speed has been shown in graphs 1 to 6.

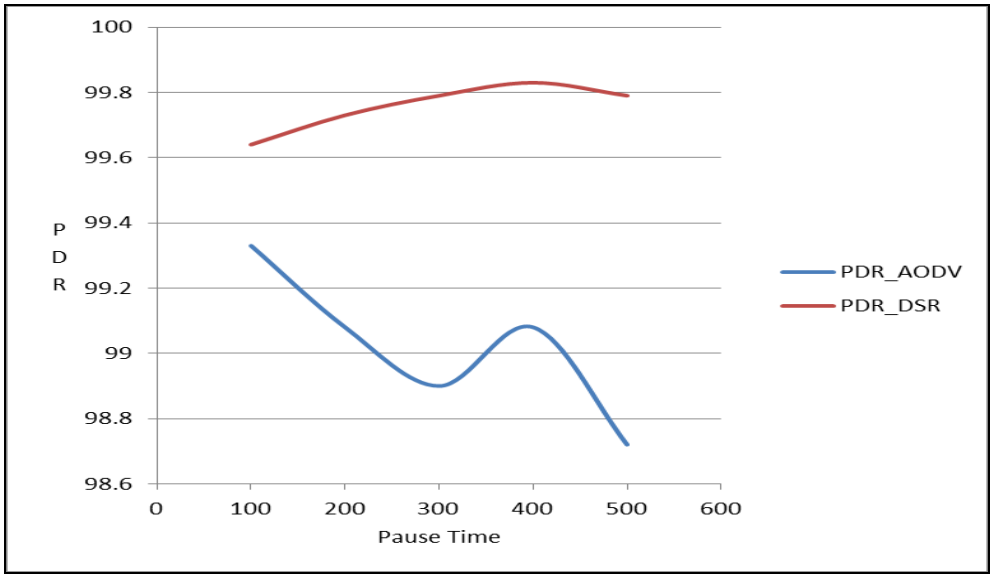

Fig 1: PDR by varying pause time for 10 nodes

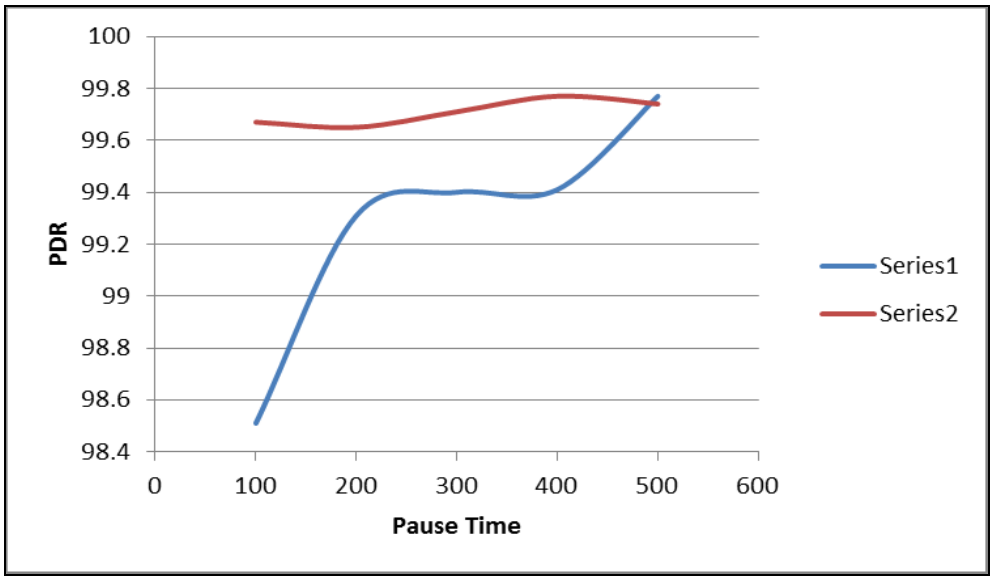

Fig 2: PDR by varying pause time for 20 nodes

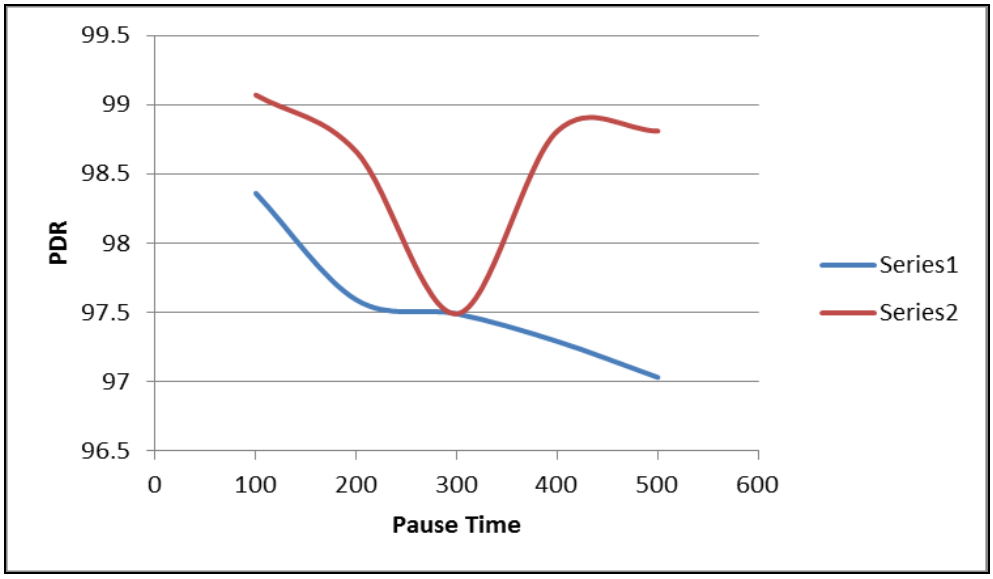

Fig 3: PDR by varying pause time for 50 node

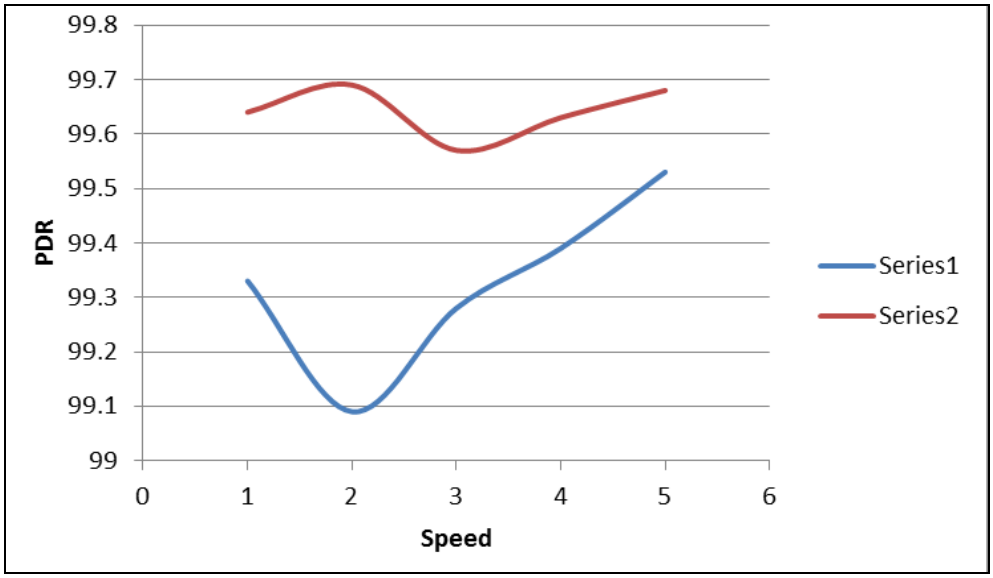

Fig 4: PDR by varying speed for 10 nodes

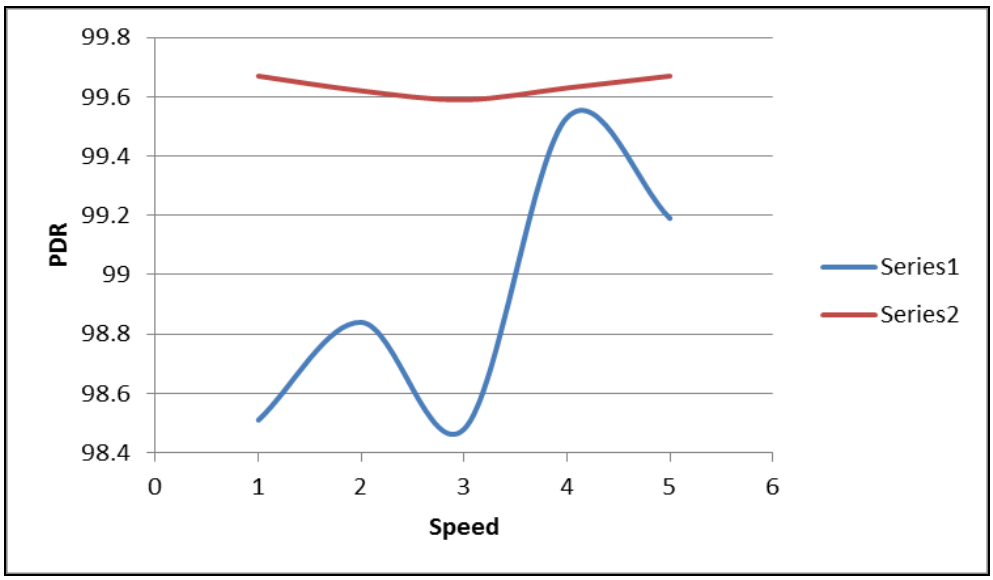

Fig 5: PDR by varying speed for 20 nodes

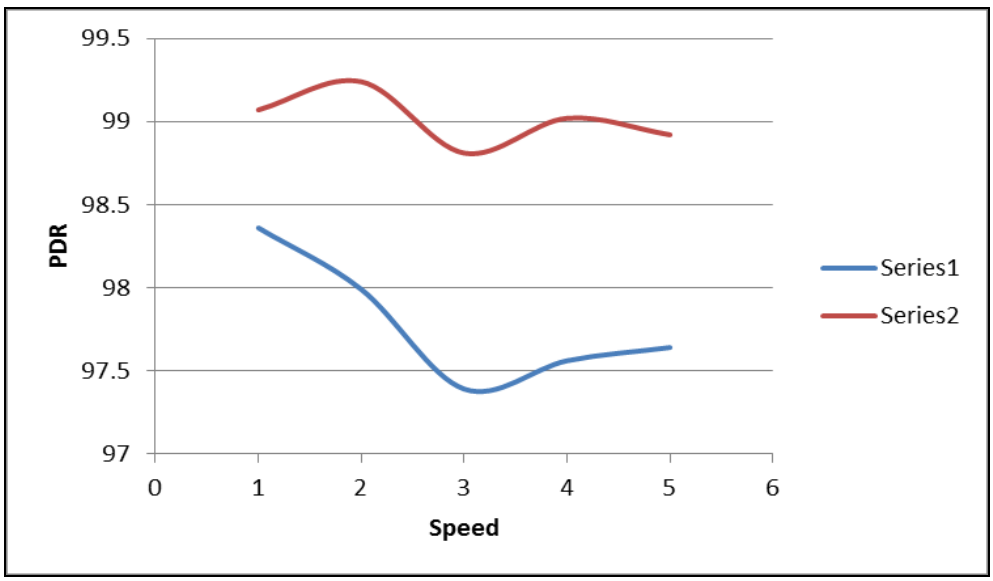

Fig 6: PDR by varying speed for 50 nodes

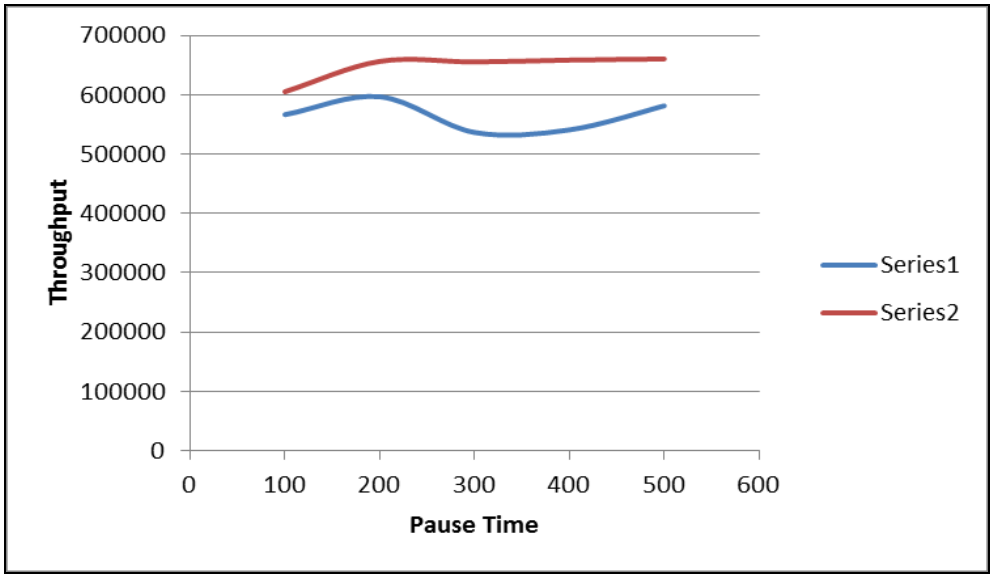

Fig 7: Throughput by varying pause time for 10 nodes

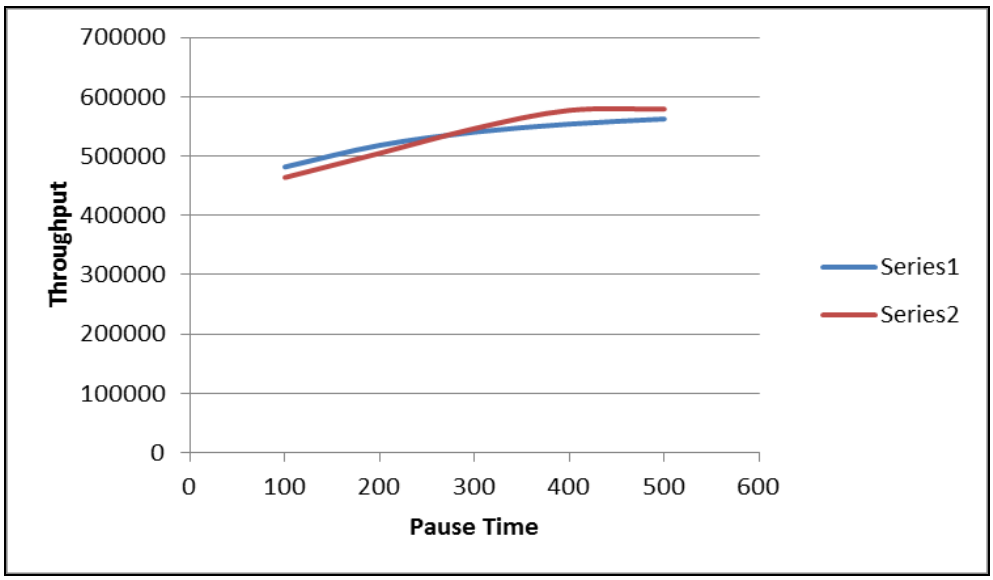

Fig 8: Throughput by varying pause time for 20 nodes

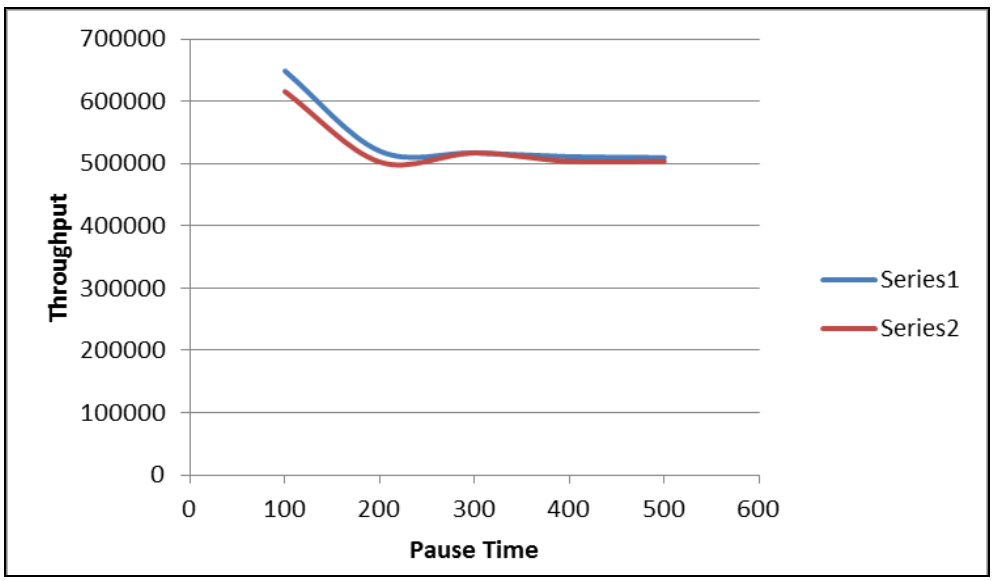

Fig 9: Throughput by varying pause time for 50 nodes

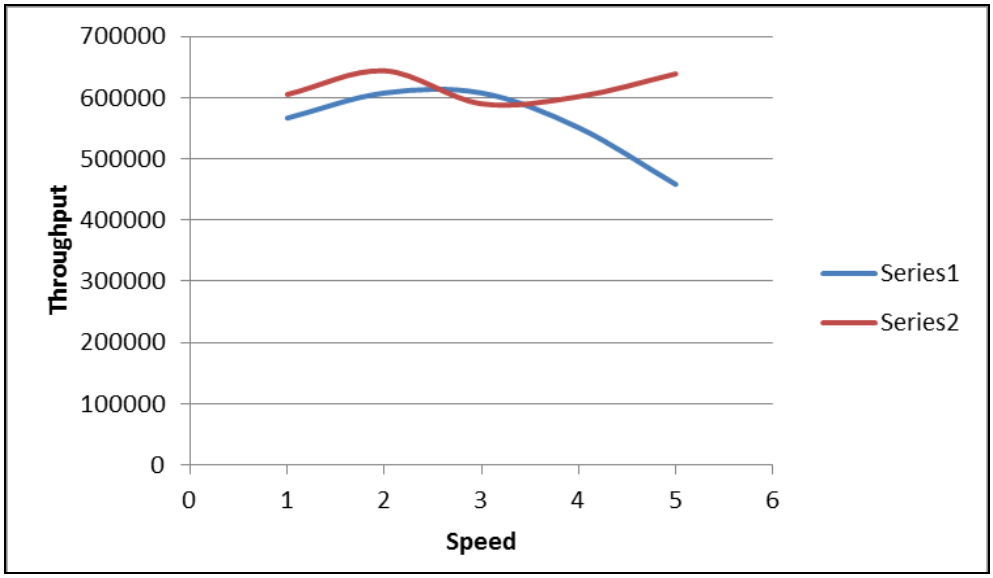

Fig 10: Throughput by varying speed for 10 nodes

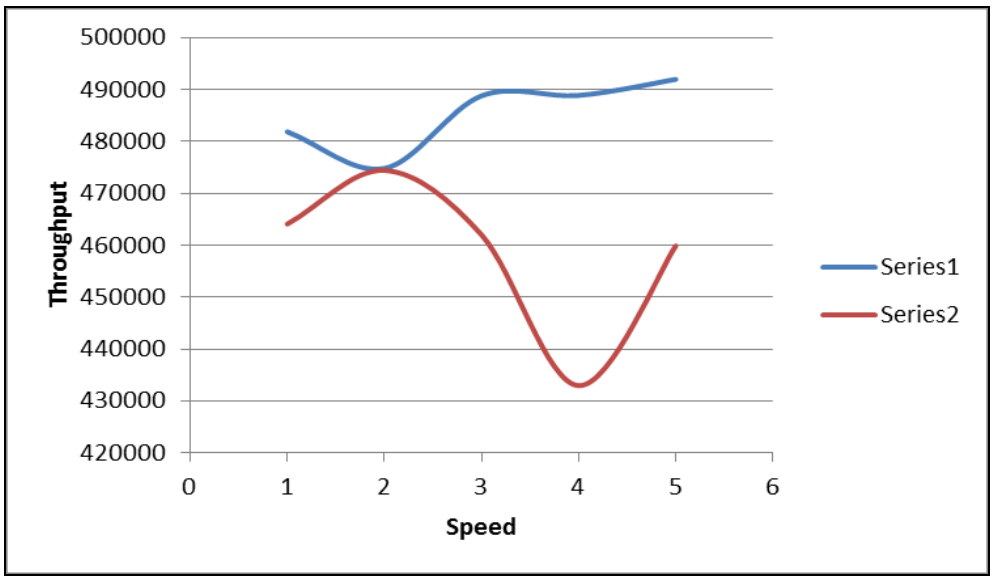

Fig 11: Throughput by varying speed for 20 nodes

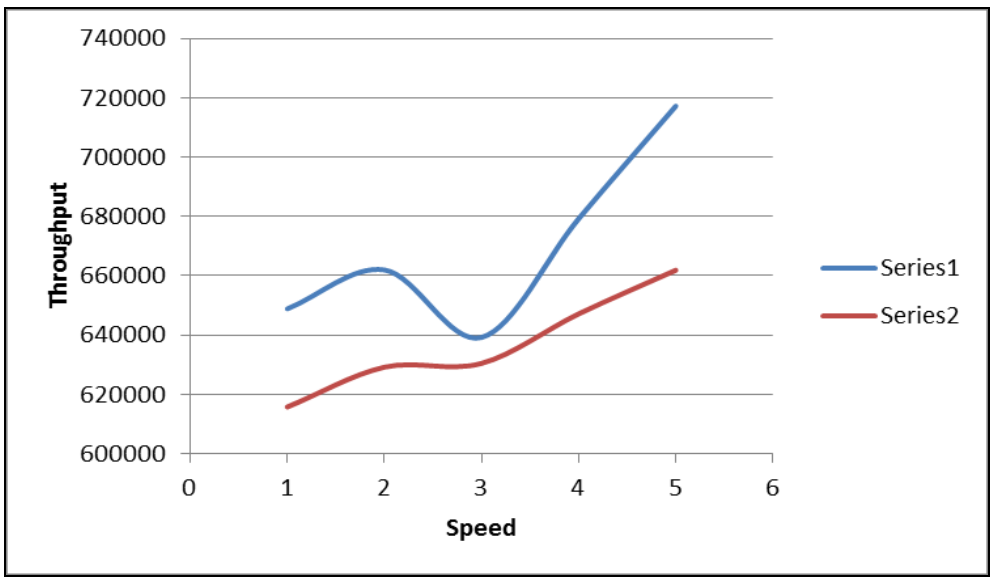

Fig 12: Throughput by varying speed for 50 nodes

In Graph 1, 3, 5 for nodes 10, 20, 50 respectively the Packet Delivery Ratio has been evaluated for DSR and AODV with the varying pause time from 100 to 500. In Graph 1 the DSR and AODV protocol are giving approximately same results when pause time is 100. DSR outperforms AODV when pause time is increased as 200 and 300 and change drastically when pause time is 500. In Graph 3 the DSR and AODV protocol gives same results when pause time is increased for Node 20. In Graph 5. The DSR and AODV protocol gives same results when pause time is 300. DSR protocol gives better results than AODV when pause time is 500.

In Graph 2,4,6 for nodes 10,20,50 respectively the Packet Delivery Ratio scale was evaluated for DSR and AODV with the varying speed from 1m/s to 5 m/s. In Graph 2 the observation reveals that the DSR protocol gives better results than AODV when speed is between 1m/s and 5 m/s. In Graph 4 DSR and AODV protocol gives same results when speed is 4 m/s. In Graph 6 also DSR and AODV protocol gives same results when speed is 4 m/s.

6. Conclusion

A detailed study has been carried out using two protocols as AODV and DSR. Two Metrics have been used as Packet delivery ratio and Throughput. Results show that in most of the cases AODV outperforms DSR. In some cases DSR performs better but in denser medium and at faster speeds ADOV always give stable and better results. Furthermore operations will be added for stable path selection and also to tackle some part of fading as well. Fading effects will also be taken care of in future work.

7. References

1. Akbani R, Korkmaz T *Raj* GVS. HEAP: A packet authentication scheme for mobile wireless networks, Wireless Networks. 2008; 6(7):1134-1150.
2. Perrig A, Canetti R, Song D, Tygar D. Efficient and secure source authentication for multicast, In Network and Distributed System Security Symposium (NDSS'01), 2001.
3. Karygiannis T, Owens L. Wireless Network Security, NIST Special Publication. 2002, 800-48.
4. William Stallings. Cryptography and Network Security: Principles and Practice, Prentice Hall New Jersey, 2003
5. Yonguang Zhang, Wenke Lee. Intrusion detection in wireless ad-hoc networks, In 6th International Conference on Mobile Computing and Networking MOBICOM'00. 2000, 275-283.
6. Kush A, Hwang C, Gupta P. Secured Routing Scheme for Adhoc Networks International Journal of Computer Theory and Engineering IJCTE. 2009; 3:1793-1799
7. Corson S, Macker J. Mobile Wireless Networking: Routing Protocol Performance Issues and Evaluation Considerations, RFC. 1999, 2501.
8. Karakehayov Z. Using REWARD to Detect Team BlackHole Attacks in Wireless Sensor Networks, Wksp. Real-World Wireless Sensor Networks. 2005, 20-21.
9. Kurosawa S, *et al*. Detecting Blackhole Attack on AODVBased Mobile Wireless Networks by Dynamic Learning Method, Proc. Int'l. J. Network Sec, 2006.
10. Zapata MG, Asokan N. Securing Ad-Hoc Routing Protocols, Proc. ACM Wksp. Wireless Sec. 2002, 1-10.
11. Dahill B, Levine BN, Royer E, Shields C. A secure routing protocol for adhoc networks‖, Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, 2001.
12. Papadimitratos P, Haas ZJ. Secure Routing for Wireless networks‖, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference CNDS, 2002.
13. Adrian Perrig, Johnson DB. Yih-Chun Hu ARIADNE: A Secure On-demand Routing Protocol for Adhoc Networks‖, ACM, Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking MobiCom, 2002.
14. Johnson DB, Maltz DA, Hu YC. The Dynamic Source Routing Protocol for Wireless networks‖, Internet Draft, MANET working group, 2003.
15. Perrig R, Canetti D, Song, Tygar D. Efficient and Secure Source Authentication for Multicast‖, In Network and Distributed System Security Symposium NDSS, 2001.
16. Perlman R. Fault-tolerant Broadcast of Routing Information‖, Computer Networks. 7, 395-405.
17. Zhou L, Haas ZJ. Securing Adhoc Networks‖, IEEE Network Magazine. 1999; 13(6):24-30.
18. Marti S, Giuli TJ, Lai K, Baker M. Mitigating Routing Misbehavior in Wireless networks‖, Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking. 2000, 255-265.
19. Bayya Arun. Security in Ad-hoc Networks‖, Computer Science Department, University of Kentucky.
20. Lakshmi K, Manju Priya S, Jeevarathinam A, Rama K, Thilagam K. Modified AODV Protocol against Blackhole Attacks in WIRELESS NETWORK", International Journal of Engineering and Technology. 2008, 2010; 2(6):444-449.
21. Sunil Taneja, Kush A. Stable and Secured Routing Strategy for MANET with SSRP, Global Journal of Computer Science and Technology. 2012; 12(4).