TRUST VALUE ALGORITHM: A SECURE APPROACH AGAINST PACKET DROP ATTACK IN WIRELESS AD-HOC NETWORKS

Rajendra Aaseri[1], Pankaj Choudhary[2], Nirmal Roberts[3]

ABV-Indian Institute of Information Technology, Gwalior, India
{jmsrdjbr[1], pschoudhary007[2], nirmal.roberts[3]}@gmail.com

ABSTRACT

Wireless ad-hoc networks are widely used because these are very easy to deploy. However, there are various security issues and problems. Two most important issues are interoperability and interaction among various security technologies which are very important to consider for configuration and management point of view. The packet drop ratio in the wireless network is very high as well as packets may be easily delayed by the attacker. Ii is very difficult to detect intruders, so it results into high false positive rate. Packets may be dropped or delayed by intruders as well as external nodes in wireless networks. Hence, there is the need of effective intrusion detection system which can detect maximum number of intruders and the corresponding packets be forwarded through some alternate paths in the network. In this paper we propose an alternate solution to detect the intruders/adversary with help of trust value. It would remove the need of inbuilt IDS in the wireless networks and result into improving the performance of WLAN.

KEYWORDS

Intrusion detection System (IDS), False Positive Rate (FPR), Intruders, WLAN, AODV.

1. INTRODUCTION

With growth of wireless local area networks [1], the dilemma of wireless security becomes more and more rigorous. There are many security issues in the wireless local area networks (WLAN) that must be considered in the formation of safe and sound WLAN. Widespread types of wireless security methods are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is solitary the slightest secure forms of security whereas WPA can be applied through firmware upgrades on wireless network interface cards designed for WEP. Wireless ad-hoc networks are self-possessed of self-governing nodes that are self-managed without any infrastructure. In this style, ad-hoc networks encompass a dynamic topology to facilitate nodes to smoothly add or delete the network components at any time. While the nodes communicate with each other without an infrastructure, they offer the connectivity by forwarding packets over themselves. To extend this connectivity, nodes bring into play some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSDV (Destination-Sequenced Distance-Vector) and DSR (Dynamic Source Routing) [2]. Since wireless ad-hoc networks involve no infrastructure [3], they are susceptible to a variety of attacks. One of these attacks is the Black Hole attack, also known as Packet Drop Attack. In the Packet Drop Attack, a nasty node absorbs the entire data packets in itself like a sink, which suck up all the incoming routing traffic into it. In this manner, all incoming packets are dropped. A malicious node exploits this vulnerability of the route sighting packets of the on demand protocols, for example AODV. In route finding progression of AODV protocol, transitional nodes are liable to find a new path to the destination. A wireless intrusion detection system (WIDS) monitors the radio range [4] used by wireless LANs, and instantaneously alerts system administrators on every occasion a suspected malicious entrance is

DOI : 10.5121/ijnsa.2013.5309

detected. Rogue campaign can spoof MAC address of an authoritative network device as its own. The prime function of a WIPS is to suppress rogue network entrance to the LAN. Both these techniques are frequently applied as a protection to the Wireless LAN. These techniques are normally used for isolation of private network from the public network. However, these are found to be not very suitable for intrusion from within the private network.

2. PREVIOUS WORK

The security exertion and security threats in the wireless networks are increasing, particularly in varied-frightening hazard, such as hacker attacks, worms, Trojans, DOS attacks etc. being serious troubles to the user. To tackle this problem, a new scheme: WBIPS (WTLS-Based IPS) replica is proposed. In this model, a coherent solitary path is build connecting each wireless terminal and its destination. Therefore an IPS engine can spot and reduce the cost for user. In WBIPS, a WTLS-based VPN (Virtual Private Network) [5] [6] is set up, and by a WTLS tunnel, wireless terminal can connect to a remote IPS engine. All traffics pass on to the engine and subsequently to their destinations.

A Lightweight WTLS-Based Intrusion Prevention Scheme is proposed by Dong Lijun, Yu Shengsheng and Xia Tao Liao Rongtao [7]. In IPS, firewall is strongly fixed with IDS, and IPS machine is positioned in same path through which all traffics pass. WTLS (Wireless Transport Layer Security) is the security layer of the WAP (Wireless Application Protocol) [8]. In this approach, the hazardous traffics can be prohibited immediately. IPS requires firewall to work with IDS. Wireless networks do not meet the extent of intensity of security as in wired networks. The entire traffics pass on to the engine and subsequently to their destinations. It gives the impression that an IPS engine is located in the path of wireless terminal's traffics. All connections are detected and checked by WBIPS.

Yaohui Wang, Xiaobo Huang (2010) proposed Analysis of Intrusion Management System Technology [9]. In this paper, the authors introduce an invasion supervision system, which can constitute for these deficiencies. Intrusion Detection System (IDS) is a fast growth kind of security object which follows the firewall. By examination of the network traffic, it discovers the network system if it has a breach of security strategy and attack symbols. It categorizes intrusion, prohibits network traffic if required and notifies in real-time. When it discovers the attack, it not only files the record and the alarm, but also alerts the administrator of dynamic protection approach to attain appropriate counter measure, and enable the emergency repair to restore the system in a sensible way.

Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang (2012) proposed some techniques for catching packet droppers and modifiers in Wireless Networks [10]. To deal with packet droppers, an extensively approved alternate approach is multipath forwarding [11], [12], [13], [14], in which every packet is forwarded along multiple surplus paths. Consequently packet drops in a few but not the all of these paths can be established. To deal with packet modifiers, most of existing countermeasures [15], [16], [17], [18] aim to filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught.

3. PACKET DROP ATTACK IN WIRELESS AD-HOC NETWOK

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for discovery of a path to the target in wireless ad-hoc networks [19]. When the source node requests to create an association with the destination node, it televises an RREQ message. In ad-hoc networks that

employ the AODV protocol, the intruder node suck up the network passage and fall all the corresponding packets. To explain the Packet Drop Attack, we include a malicious node that demonstrates Black Hole activities in the set-up. We illustrate the packet drop attack with help of given scenario shown in Figure 1. We suppose that Node 3 is the malicious node. When Node 1 televise the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that contain the maximum sequence number of Node 4, as if it is coming from Node 4.
Node 1 presumes that Node 4 is following Node 3 with 1 hop and discards the recently arrived RREP packet coming from Node 2. Subsequently, Node 1 begin to discharge its data packet to the node 3 expecting that these packets will arrive at Node 4 but Node 3 will slump all data packets. In a Packet Drop Attack, after a while, the starting nodes realize that there is a linkage fault since the acceptance node refusing to transmit TCP ACK packets. If it dispatch away fresh TCP data packets and find out a fresh route for the target, the malicious node still handle to cheat the sending node. If the sending node releases UDP data packets, the difficulty is not identified since the UDP data connections do not hang around for the ACK packets.

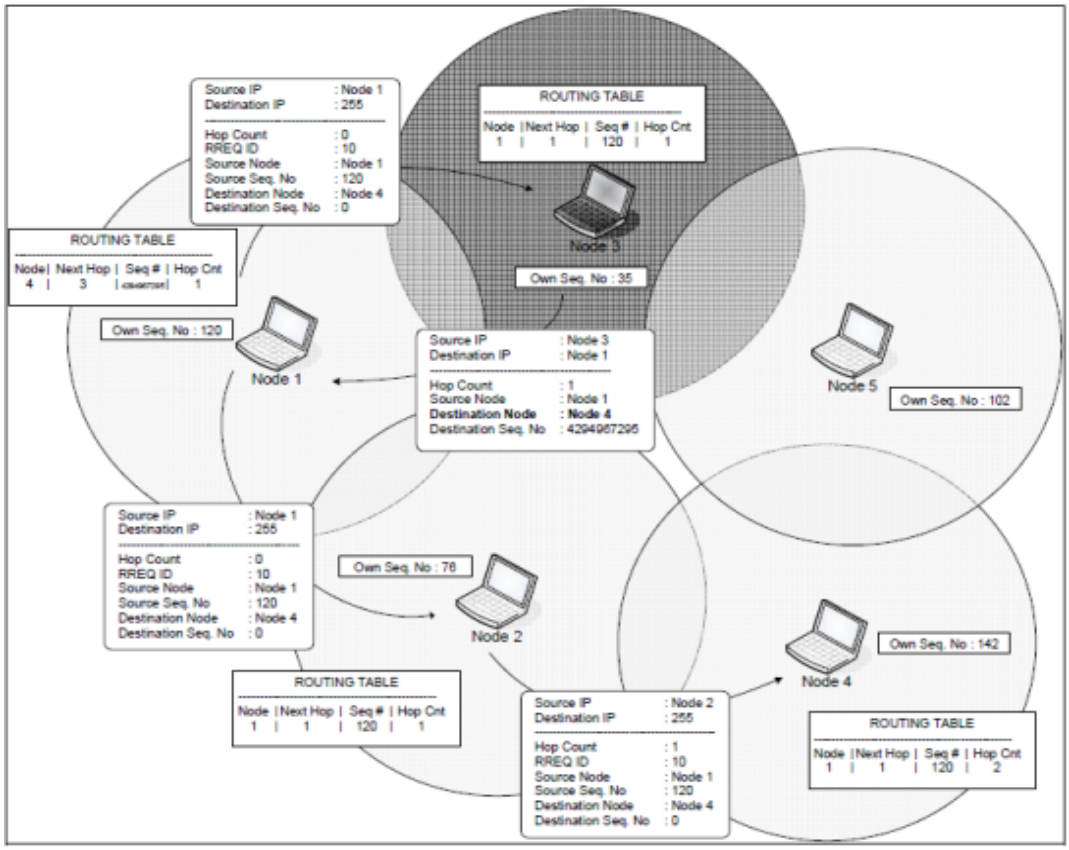

Figure 1: Demonstration of Packet Drop Attack [19]

4. PROBLEM FORMULATION AND PROPOSED SCHEME

Wireless networks are very easy to deploy because there is no need to establish any physical path. This feature of wireless network results into birth of various attacks. In the Packet drop attack, the attacker targets some nodes in the wireless network and then drop the packets sent towards the intended nodes. Attackers try to drop/delay the packets in the routine manner so it's very difficult to detect. The packet drop will further results into the high false positive rates and ultimately

breaks the security of wireless networks. So, our problem is to detect the Packet drop attack and try to reduce the packet drop ratio so that it will result into law false positive rates.

4.1 PROPOSED ALGORITHM

If the number of packet drop nodes increases then the data thrashing would also likely to be boost [5]. A malicious node can initiate the following two attacks:

PACKET SINKING: A malicious node slump all or a few of the packets that is believed to be forward. It can also sink the data produced by itself on behalf of some malicious intention for instance.

PACKET AMENDMENT: A malicious node alters the entire or a few of the data packets that is made-up to forward. It can also modify the data it produce to defend it from being recognized or to lay blame on former nodes.

In previous Black hole detection techniques, black hole node is randomly chosen based on the number of packet dropped. So, sometime legitimate user also treated as the intruders or attacker. It will result into high false positive rate and it violates the security of wireless networks.

TRUST VALUE ALGORITHM: The proposed algorithm is based on the trust values of individual nodes. Initially, all the nodes of wireless ad-hoc network have zero trust value. The algorithm comprises the following steps:

[A] Initialization:

1. Trust values of all the participating nodes are initializing with zero.
2. Initialize the threshold value of the trust value with 100.
3. Assumption: 1 trust value = 10 packets dropped.

[B] Updating of trust values:

1. If the packets are correctly transmitted from one node to another node:
   (a) If the correctly transmitted number of packets is between 1 to 10, then trust values of the respective nodes will be incremented by one time.
   Updated trust value = old trust value + 1;
   (b) If the correctly transmitted number of packets are greater than 10, then the updated trust value will be:
   Updated trust value = old trust value + (correctly transmitted packets / 10);

2. If the packets are dropped/delayed :
   (a) The number of dropped or delayed packets is between 1 to 10, then trust value of that particular node is decremented by one.
   Updated trust value = old trust value – 1;
   (b) The number of dropped or delayed packets are greater than 10, then trust value of that particular node will be,
   Updated trust value = old trust value **–** (Packet dropped or delayed / 10);

3. If the trust value of particular node is negative, then print “Invalid node”.

[C] Isolating the Packet drop node from the network:

1. If (Updated trust value <<< Threshold trust value)
   Then the particular node is treated as malicious node (Black hole node)
2. If (Updated trust value > Threshold trust value)
   Then the particular node is treated as legitimate node.
3. Stop comparing the trust values of nodes with threshold value.

In our approach, we detect the black hole node based on the trust values (Proposed trust value algorithm). We used Traffic pattern Analysis Techniques and associate trust values with each wireless nodes. Initially, all nodes has 'zero' trust value. If the particular node is not involving in packet drops, then each time the trust value of corresponding node will increase by 1.

When a particular node reaches its trust value equal or more than threshold value then that node will be treated as legitimate node for further communication. In this manner we calculated trust value of each and every node. If particular node is not attaining its trust value to the threshold then it will be treated as the packet dropper/modifier node and it will be called as illegal node for further communication. Reduction in the packet drop ratio will result into the low false positive rates and ultimately it will result into the improved security of WLAN.

5. SIMULATION AND EXPERIMENT

In this effort, we have tried to assess the special effects of the Packet Drop attacks in the Wireless Ad-hoc Networks. To attain this we have replicated the wireless ad-hoc network set-up which contains packet drop node using NS2 Network Simulator program. To create the packet drop node in a wireless ad-hoc network we have employed fresh protocol that jump down data packets after be a magnet for them to itself.

TABLE 1: SIMULATION PARAMETERS

Parameter	**Specification**
Simulation tools Used	NS2 Network Simulator (NS 2.35), Exata
Simulation Time	10 sec, 20 sec
Number of Nodes	20,40,60,80,100
Transmission Range	250 m
Maximum Speed	0-22 m/sec
Application Traffic	CBR(Constant Bit Rate) [20]
Packet Size	512 Bytes
Node Mobility Model	8 Packets/sec
Protocol	AODV
Number of runs	12
Threshold trust value	100

To obtain correct results from the simulations, we applied UDP protocol. The source node remains on carriage out UDP packets, although the nasty node goes down them, while the node terminates the link if it makes use of TCP protocol. As a result, we may possibly examine the connection flow between sending node and receiving node throughout the simulation.

5.1 SIMULATION SET UP AND NETWORK SCENARIO

NS2 Simulator generates a tcl (Tool Command Language) file. On running the tcl file, it results into two more files, first the trace file which contains all the information regarding the network and second the nam (Network animator) file which is a visual aid showing how packets flow along the network and shows the Virtualization of the network corresponding to the trace file. All routing protocols in NS2 are mounting in the directory of “ns-2.35”.

We begin the simulation by duplicate AODV protocol in this directory and alter the name of directory as “packetdropaodv”. We create a tiny size network that has seven nodes and generate a UDP link connecting Node 2 and Node 5, and affix CBR (Constant Bit Rate) function that produce constant packets in the course of the UDP connection. Duration of the scenarios is 20 seconds and the CBR connections taking place at time equals to 1.0 seconds and carry on until the end of the simulation.

5.2 EVALUATION OF SIMULATION

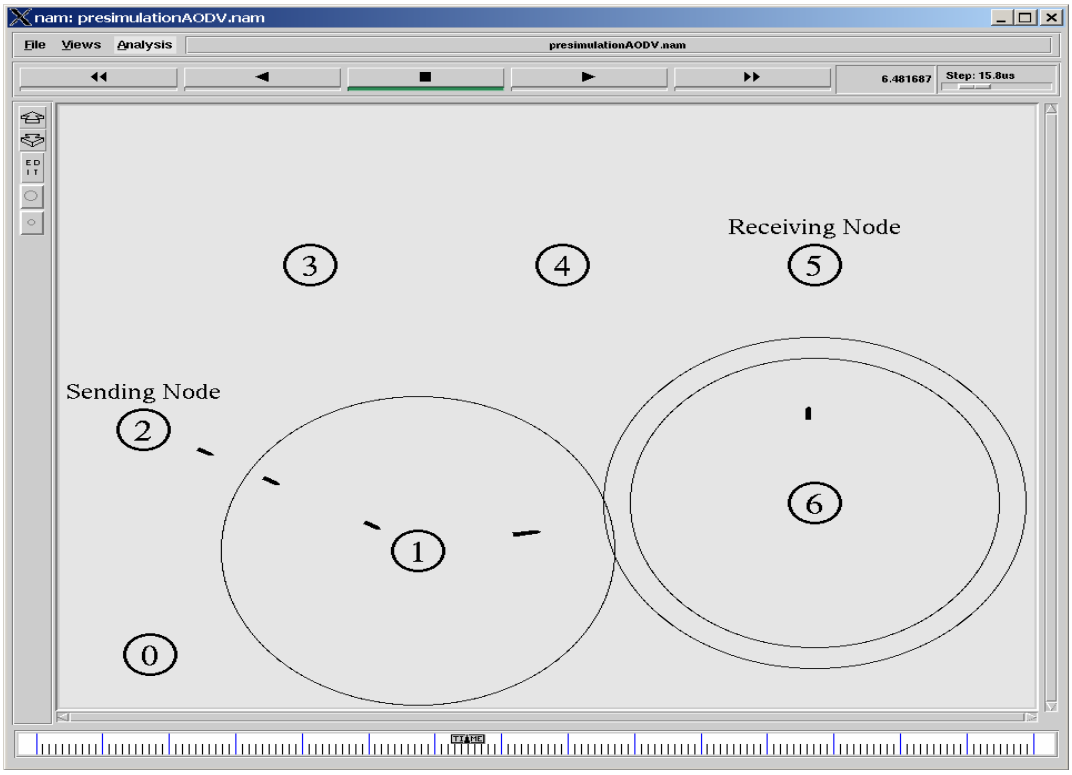

Figure 2: Data stream between Node 2 and Node 5 through Node 1 and Node 6

We cannot easily see the effects of the Black Hole AODV Node in the large number of Nodes and connections, we will carry out in the actual simulation, and we had to test the implementation in a small sized simulation that has a small number of nodes.

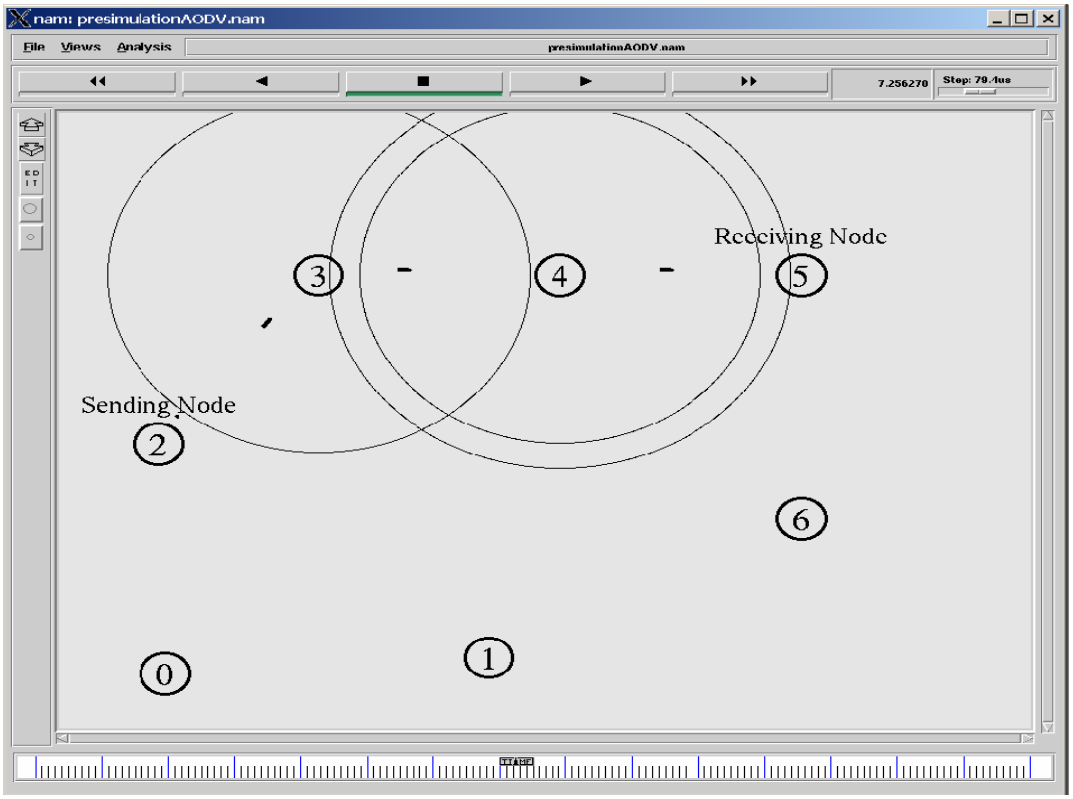

Figure 3: Data stream between Node 2 and Node 5 through Node 3 and Node 4

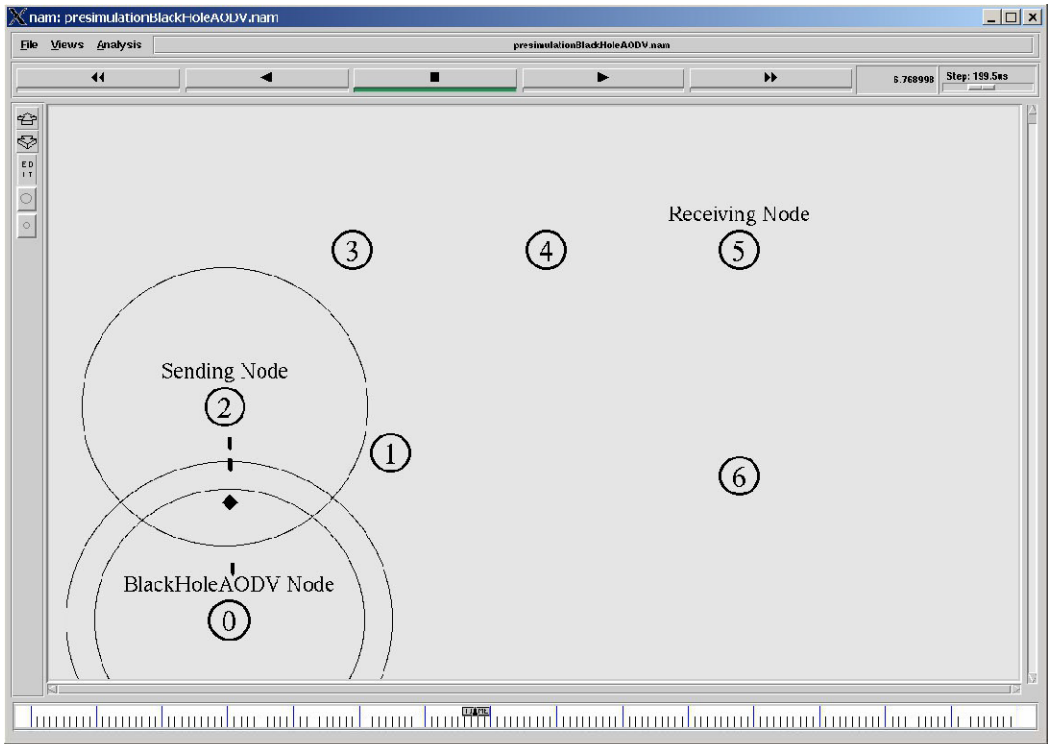

Figure 4: Node 0 (Black Hole Node) suck up the connection between Node 2 to Node 5

6. ANALYSIS OF SIMULATION RESULTS

We simulated 10 different network scenarios having different number of nodes. We observe the simulation results to get the values of various network parameters like throughput, Packet drop ratio (PDR), Packet delivery ratio (PDLR), Average trust value and false positive rate (FPR). Various graphs are plotted to observe the relationship between these parameters.

TABLE 2: EXPERIMENT DATA WITH 10 DIFFERENT SCENARIOS

Scenario	**Nodes**	**Throughput** (mbps)	**FPR**	**PDR**	**Avg. trust value**	**PDLR**
1	10	2.793	0.013	0.013	91.42	0.987
2	20	2.923	0.042	0.019	85.63	0.967
3	30	2.897	0.061	0.027	81.03	0.943
4	40	2.453	0.097	0.074	76.45	0.912
5	50	2.307	0.153	0.156	72.09	0.893
6	60	2.109	0.196	0.162	71.73	0.796
7	70	2.908	0.173	0.159	72.95	0.776
8	80	2.003	0.237	0.204	69.78	0.709
9	90	1.459	0.214	0.193	70.05	0.698
10	100	1.763	0.349	0.297	63.50	0.635

PDLR: Packet delivery ratio PDR: Packet drop ratio FPR: False positive rate

Figure 5 shows the variation of throughput with the packet drops. We observe that as the number of packet drop increases, corresponding throughput decreases. Figure 6 shows the variation of throughput with the false positive rate (FPR). Throughput shows the tendency to reduce with increasing false positive rate (FPR). Figure 7 shows the variation of throughput against packet delivery ratio. Here, the throughput increases with increasing packet delivery ratio. Figure 8 shows that the FPR also increases as the PDR increases.

Figure 9 shows the effect of PDR on the trust values. It clearly implies that as the PDR increases the trust value deceased in an almost linear way. The node which acquires its trust value equal to or more than the threshold value is considered a legitimate node. Figure 10 shows the effect of FPR on the trust values. Here, FPR decreases with increasing the trust values in an almost linear way. As the average trust value tends to threshold value, it results into low false positive rate. i.e. there is high chance of detection of the malicious node and ultimately it will result into the improved security of WLAN.

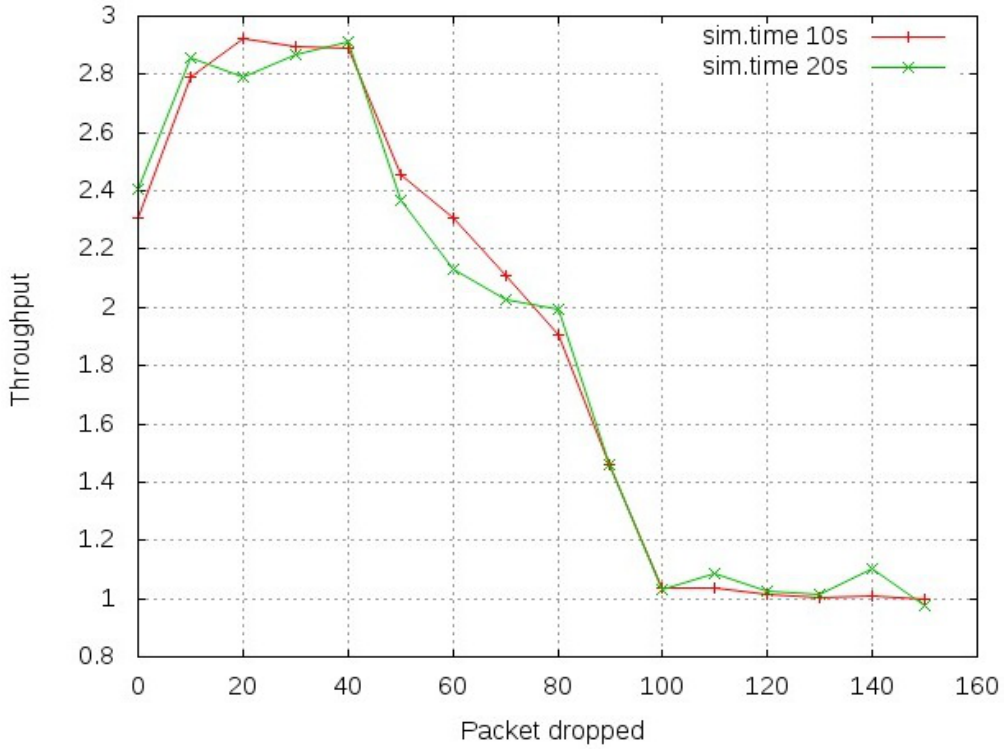

Figure 5: Throughput Vs Packet dropped

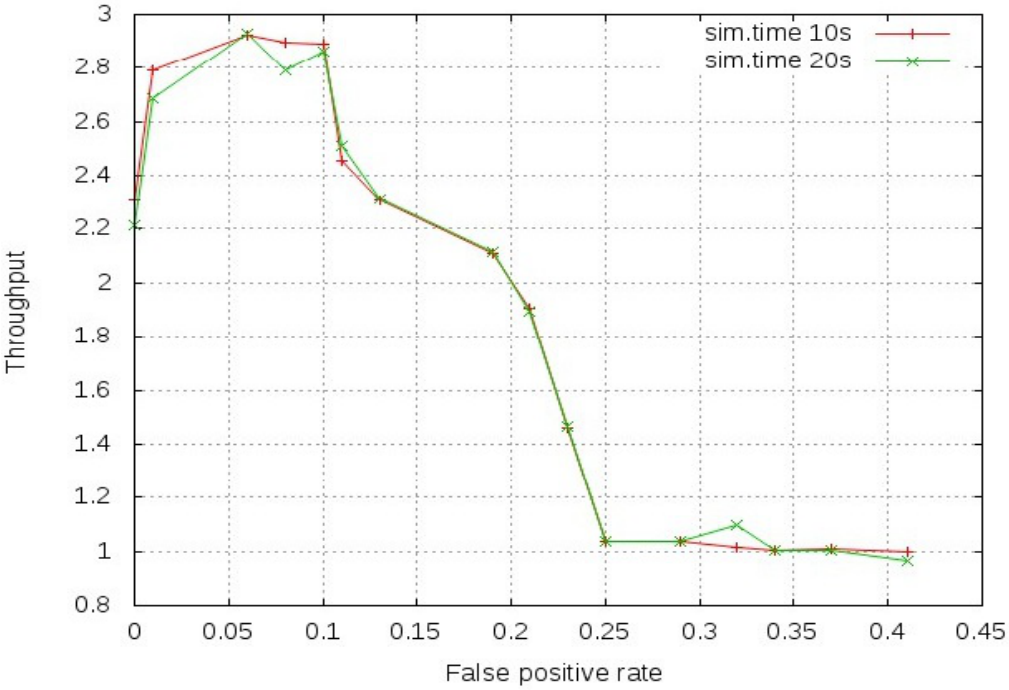

Figure 6: Throughput Vs False Positive Rate

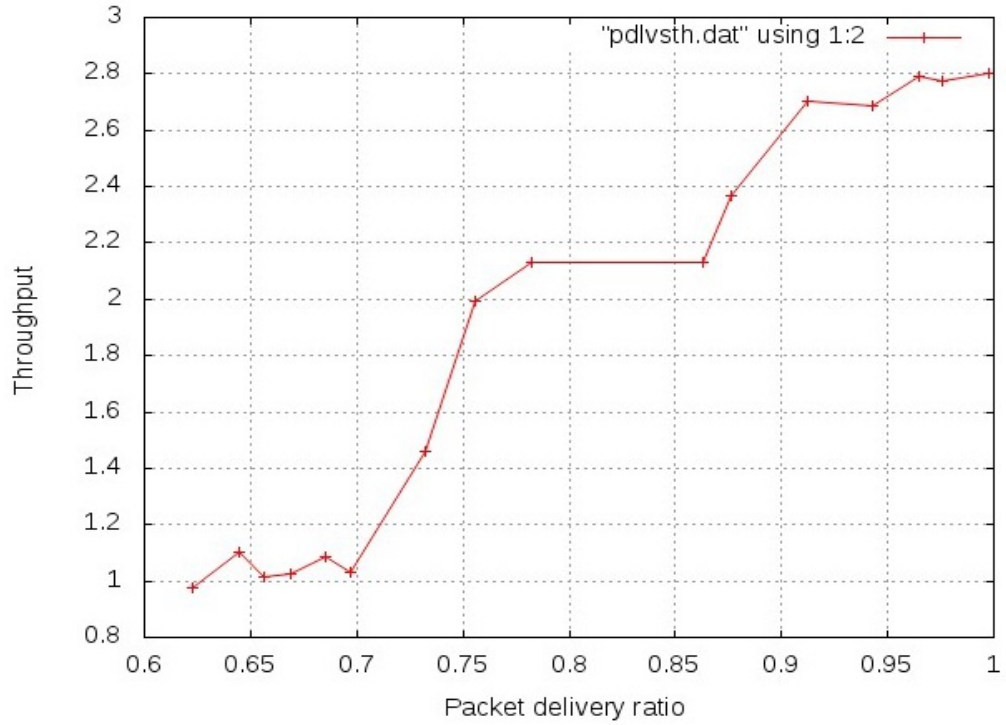

Figure 7: Throughput Vs Packet delivery ratio

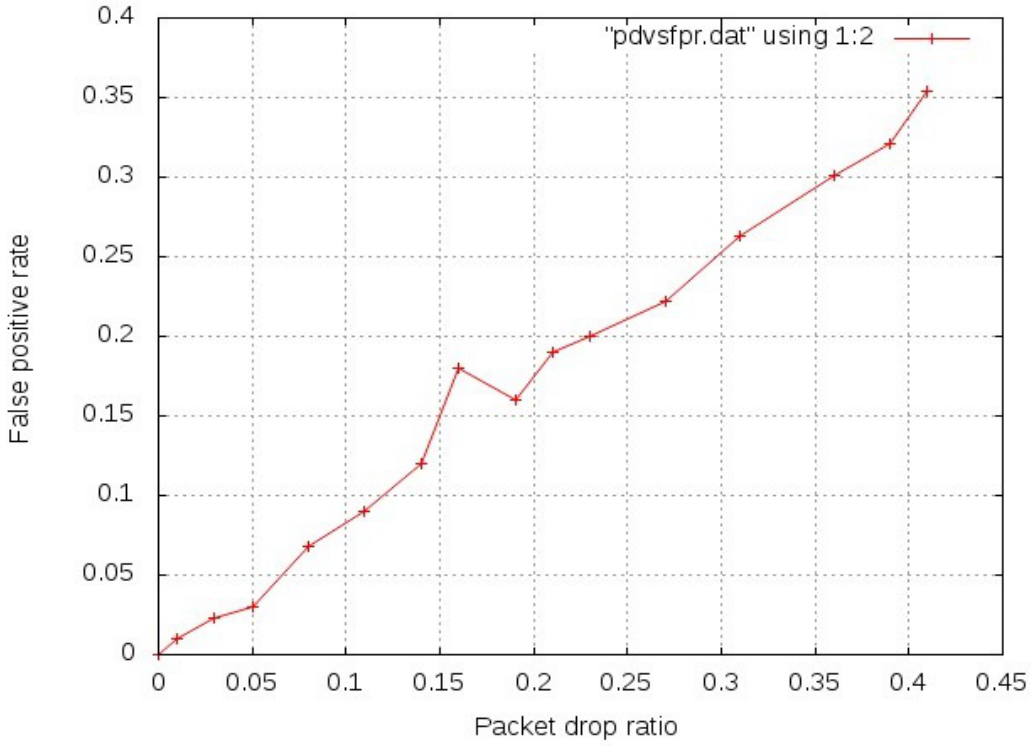

Figure 8: False Positive Rate Vs Packet Drop Ratio

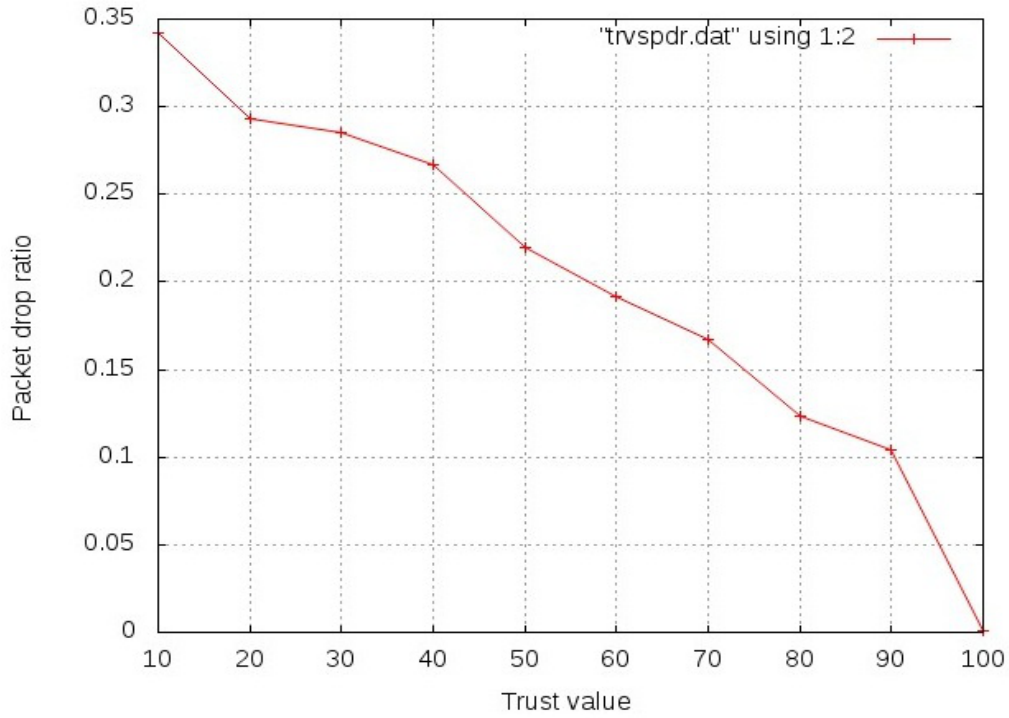

Figure 9: Packet Drop Ratio Vs Trust value

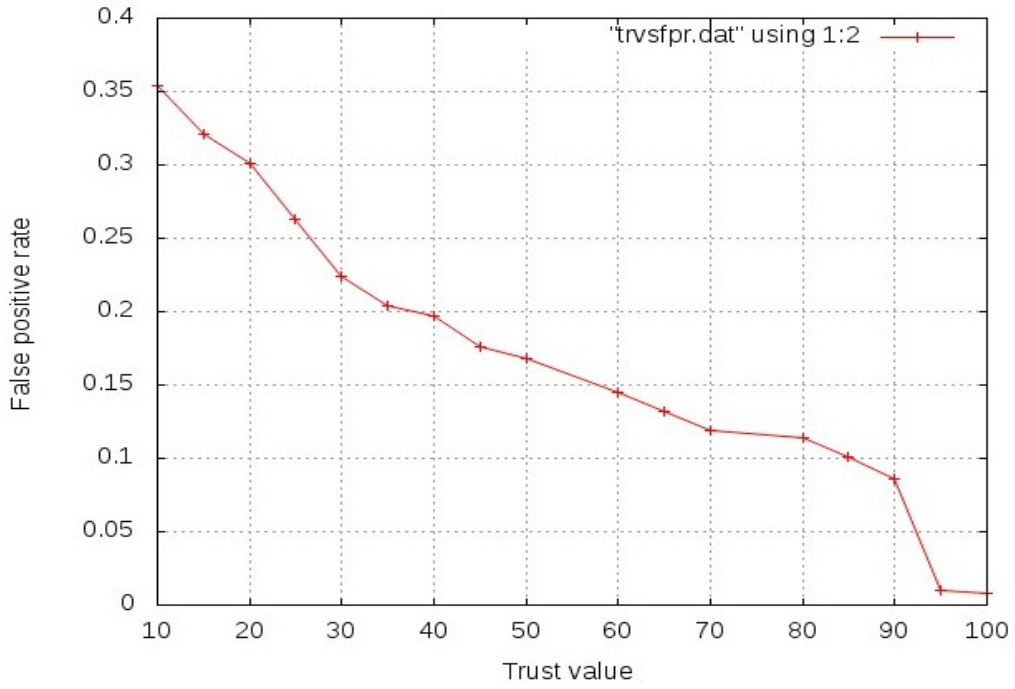

Figure 10: False Positive Rate Vs Trust value

7. CONCLUSIONS

After simulating the packet drop attack, we observe that the packet loss is higher in the ad-hoc network. If the number of packet drop Nodes is enlarged then the data loss would also be likely to mount. AODV network has generally 5.79% data loss and if a packet drop node is introduced in this network, data loss is enlarged to 87.45 %. As 5.79 % data loss previously survives in this data traffic, Packet drop node boosts this data loss by 81.66 %. Malicious nodes, in the wireless ad-hoc networks are detected on the basis of their corresponding trust values with assist of our proposed trust value algorithm. Our Approach can detect malicious node with 87% of success which further results into data security (decrease in data loss) by 75.69%. So, Our Approach solves the problem of Packet drop attack with 92% of the success which is far better than the earlier prevention technique to packet drop attack.

8. FUTURE WORK

In our work, we simulated the Packet Drop Attack in the Wireless Ad-hoc Networks using AODV routing protocol and examine its influence. Similarly, other routing protocols could be simulated as well. Simulation results for different routing protocols are likely to present varied, interesting and thought provoking conclusions. Thus, the best routing protocol for minimizing the Packet Drop Attack may be determined.

With help of our proposed Trust Value Algorithm the black hole node can be detected based on the trust values which will result into the low false positive rates. We used UDP connection to calculate the packets at sending and receiving nodes. If we had used the TCP connection among nodes, the sending node would be the end of the connection, since ACK packets do not arrive at the sending node. The discovery the black hole node with connection oriented protocols could be another future work.

8. REFERENCES

[1] Yong Yu; Qun Wang; Yan Jiang, "Research on security of the WLAN campus network," *E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on* , vol.2, no., pp.175,178, 17-18 April 2010.

[2] Hemalatha, S.; Mahesh, P.C.S.; Rodrigues, P.; Raveendiran, M., "Analysing cross layer performance based on Sinking and Collision Behaviour attack in MANET," *Radar, Communication and Computing (ICRCC), 2012 International Conference on* , vol., no., pp.77,82, 21-22 Dec. 2012.

[3] Ning Song; Lijun Qian; Xiangfang Li, "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," *Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International* , vol., no., pp.8 pp.,, 4-8 April 2005.

[4] Chaudhari, B.; Gothankar, P.; Iyer, A.; Ambawade, D.D., "Wireless network security using dynamic rule generation of firewall," *Communication, Information & Computing Technology (ICCICT), 2012 International Conference on* , vol., no., pp.1,4, 19-20 Oct. 2012.

[5] R. Cohen. “On the establishment of an access VPN in broadband access networks”. Communications Magazine, IEEE, 41(2): 156-163. 2003.

[6] Runguo Ye, Yangjun Feng, Shuyao Yu, Cheng Song. “A Lightweight WTLS-based Mobile VPN Scheme”. Microelectronics & Computer. 2005. Vol.22. No.4.. pp 126-133.

[7] Dong Lijun; Yu Shengsheng; Xia Tao; Liao Rongtao, "WBIPS: A Lightweight WTLS-Based Intrusion Prevention Scheme," *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on* , vol., no., pp.2298,2301, 21-25 Sept. 2007.

[8] WAP Forum, “Wireless Application protocol-Wireless Transport Layer Security Specification”. Version 18-Feb-2000.

[9] Yaohui Wang; Xiaobo Huang, "Analysis of Intrusion Management System Technology," *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on* , vol., no., pp.1,3, 23-25 Sept. 2010.

[10] Guiling Wang, Wensheng Zhang, Jinsook Kim, Taiming Feng, Chuang Wang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 5, pp. 835-843, May, 2012.

[11] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.

[12] V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005.

[13] M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, "Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks," Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006.

[14] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad HocNetworks, vol. 5, no. 1, pp. 87-99, 2007.

[15] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, 2004.

[16] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[17] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), 2005.

[18] Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2006.

[19] Dokurer, S.; Erten, Y.M.; Acar, C.E., "Performance analysis of ad-hoc networks under black hole attacks," *SoutheastCon, 2007. Proceedings. IEEE* , vol., no., pp.148,153, 22-25 March 2007 doi: 10.1109/SECON.2007.342872.

[20] Liang Zhao, Ahmed Y. Al-Dubai, and Imed Romdhani. 2010. Novel QoS-Aware Gateway Centralized Multi-hop Routing for Wireless Mesh Networks. In Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology (CIT '10). IEEE Computer Society, Washington, DC, USA, 336-342. DOI=10.1109/CIT.2010.500 http://dx.doi.org/10.1109/CIT.2010.500.