POTENTIAL SECURITY ATTACKS ON WIRELESS NETWORKS AND THEIR COUNTERMEASURE

Sreedhar. C[1], Dr. S. Madhusudhana Verma[2] and Dr. N. Kasiviswanath[3]

[1]Department of CSE, G. Pulla Reddy Engineering College, Kurnool, India
csrgprec@gmail.com
[2]Professor, Department of OR & SQC, Rayalaseema University, Kurnool, India
seeverma@rediffmail.com
[3] Professor, Department of CSE, G. Pulla Reddy Engineering College, Kurnool, India
nkasiviswanath@yahoo.com

ABSTRACT

The security of wireless networks has been a constant topic in the recent years. With the advance of wireless networks, building reliable and secured communication is becoming extremely important. Wireless security is a mechanism of preventing unauthorized access or damage to computers using wireless networks. A mobile ad-hoc network (MANET) is a self-organizing system of mobile nodes that communicate with each other through wireless links with no fixed infrastructure or centralized administration. This paper presents potential security attacks on Ad-hoc On-demand Distance Vector (AODV) routing protocol and their countermeasure. IETF standardized AODV and considered as one of the most popular and promising on-demand routing protocols because of its lower network overhead and algorithm complexity. AODV protocol does not store all the routing information in its routing table and this causes potential security threat to the wireless networks. In this paper, we consider various known security attacks and in- specific blackhole attack on AODV and propose a countermeasure to thwart blackhole attack.

KEYWORDS

MANET, Security, blackhole attack, AODV.

1. INTRODUCTION

MANETs consist of mobile nodes interconnected by multi hop communications paths. A MANET consists of mobile nodes, which are free to move at any speed in any direction and are self-organized. Vehicles and humans can be internetworked in areas without any preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [1]. MANET is a self-configuring network of mobile routers connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily. Figure 1 illustrates the flowchart which depicts the working of any general ad-hoc network. MANET routing protocols can be classified into demand-driven, table-driven and hybrid routing protocols. Examples of on-demand-driven protocols are Ad-hoc On-Demand Distance Vector (AODV) [2] and Dynamic Source Routing (DSR) [3]. Table-driven protocols attempt to maintain consistent, up to date routing information in routing tables on every node. Hybrid routing protocols combines features of table-driven and on-demand. Examples of table-driven protocols are Destination Sequenced Distance Vector (DSDV) [4], Optimized Link State Routing (OLSR) [5] and wireless routing protocol (WRP). In MANET, security emerges as a central requirement due to its characteristics of changing network topology and lack of central authority. Although there exist a large number of MANET routing protocols, most of them were designed without any security considerations and in general it is assumed that all nodes are friendly. Besides, the resource constraints (both computation and bandwidth) of MANET put up great difficulties over

DOI : 10.5121/ijcsit.2010.2506

the deployment of security. The dynamic topology, lack of a fixed infrastructure and the wireless nature make MANETs susceptible to the security attacks. To add to that, due to the inherent, severe constraints in power, storage and computational resources in the MANET nodes, incorporating sound defence mechanisms against such attacks is also non-trivial. Therefore, the traditional security mechanisms and protocols – including those for the wired networks - are not directly applicable and require a careful relook [6].

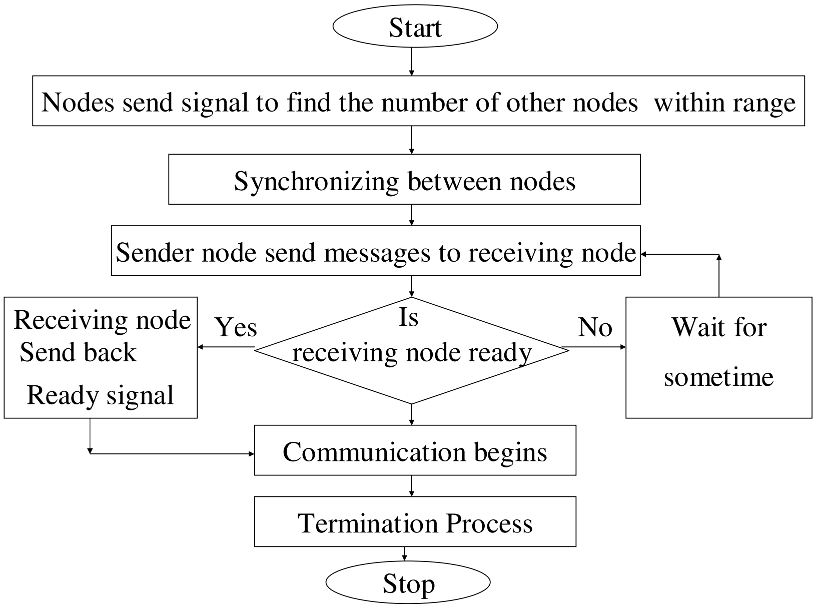
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Is receiving node ready
Yes
No
Receiving node Send back Ready signal
Wait for sometime
Communication begins
Termination Process
Stop

Figure 1. General ad-hoc network communication

Any routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

- *Confidentiality*: Protection of any information from being exposed to unintended entities. In ad-hoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.

- *Availability:* ensures that network services are provided as supposed to be. In an ad-hoc network without protection of proper security mechanisms, its service performance and availability can be easily compromised. For example, signal jamming at the physical and media access control layers can seriously interfere with communications or even bring down the physical channels. A malicious or selfish node can also disrupt routing services, which may result in network partition

- *Authentication*: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

- *Integrity*: Message being transmitted is never altered.

- *Non-repudiation:* Ensures that sending and receiving parties can never deny ever sending or receiving the message.

2. SECURITY CHALLENGES IN ROUTING PROTOCOLS

MANETs are networks with no fixed infrastructure and network functions are carried out by all available nodes, which are highly mobile and have constrained power resources [7]. Consequently, MANETs has increased sensitivity to node misbehavior [7] [8] [9] [10]. There are two sources of attacks related to node misbehavior in mobile ad hoc networks [11]. The first is *external attacker*, in which unauthenticated attackers can replay old routing information or inject false routing information to partition the network or increase the network load. The second is *internal attack*, which comes from the compromised nodes inside the network. Since compromised nodes can be authenticated, internal attacks are usually much harder to detect and can create severe damage.

MANETs suffer from all the vulnerabilities that their wired counterparts encountered. An adversary may launch various attacks ranging from passive eavesdropping to active interference such as packet modification and fabrication, traffic jamming, denial-of-service (DoS), message reply and various other attacks. Due to the characteristics of MANETs, some of these vulnerabilities are aggravated in a wireless context. Eavesdropping is generally easier in MANETs than in the internet due to the open nature of the communication medium in MANETs. Passive attacks are by nature difficult to detect. All the above security mechanisms must be implemented in any ad-hoc networks so as to ensure the security of the transmissions along that network. Thus whenever considering any security issues with respect to a network, we always need to ensure that the above mentioned 5 security goals have been put into effect and none (most) of them are flawed. In MANETs, attacks can be done by a malicious node using different ways. For example sending fake messages multiple times, fake routing information, and advertising fake links to disrupt routing operations. MANETs does not have fixed boundaries and range of network transmission may exceeds the area where the network is deployed exposing the network to numerous attacks, which are not easily detected such as eavesdropping. Hence security in MANETs is a permanent need and part of the communication. In MANETs, there is no centralized authority, responsible of the distribution of cryptographic keys or the management of the Public Key Infrastructure, as in conventional networks. Any routing protocol designed for MANETs must include implementation of security during design. All the widely used current MANET routing protocols do not consider security issues and assume that all the network's nodes fairly participate in the routing operation without any malicious intention which is not always true in reality, in addition, outsider intruders can perform attacks such as DoS attacks, data modification or simply eavesdrop the exchanged data.

We present the security risks faced by MANET routing in which the exchanged messages are exposed in a MANET through simulation. The number of nodes we have considered for simulation are 25 and 50 mobile nodes in the area of 690 * 690 sq.mt. Around 10% of them to be attackers are assumed, which are performing data modification attack. We have also used some CBR (Constant Bit Rate) connections with packet length of 512 bytes to emulate traffic over the network.

Table 1. Simulation Parameters.

Parameters	Values
Network size	690*690 m^2
Number of Nodes	30, 60
Max speed	20 m/s
Wait Time	50 s
CBR connections	4,5,6,7,8
Routing protocol	AODV
Number of attackers	10%
Simulation time	600s

Table 1 describes the various simulation parameters considered. We have used as simulation tool ns2 [12], which is recognized as one of the most powerful tool for wireless and wired networks simulations.

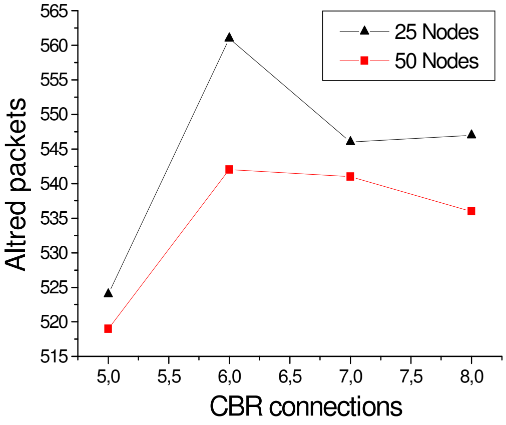

Figure 2. Number of altered packets forwarded by each node.

Securing routing protocols is one of these challenging tasks, since security is not natively implemented in ad hoc routing, and the extensions given in literature are complex and vulnerable against several attacks. Figure 2 describes the average number of altered packets forwarded by each mobile node in the network with the absence of any security or intrusion detection mechanism. The number of altered packet is very high according to the number of CBR connections which is only five connections, we observe also that the number of altered packets gets high when the number of nodes is small this is because each node in a small network forward more data, which gives to the attacker more opportunity to alter and modify packets. From these simulations we can predict the potential danger that makes any attacker in the network, since each node in the network forwards a great portion of data giving him the ability to control and eavesdrop the majority of the exchanged data over the network. The following subsection describes various known security attacks on MANETs

2.1. Attack using Modification

Conventional routing protocols for MANET neglect that intermediate mobile nodes alter maliciously the control fields of messages to distribute falsified values. Hence it makes no difficult for malicious nodes to compromise the integrity of routing message and modify routing information, which cause network traffic to be dropped, redirected to a different destination, or take a longer route to the destination increasing communication delays. An example is for an attacker to send fake routing packets to generate a routing loop, which causes packets to pass through nodes in a cycle without getting to their actual destinations, consuming energy and bandwidth. Similarly by sending forged routing packets to other nodes, all traffic can be diverted to the attacker or to some other node. The idea is to create a black hole by routing all packets to the attacker and then discarding it. As an extension to the black hole, an attacker could build a grey hole, in which it intentionally drops some packets. The other type of modification attack is the creation of wormhole attack in network. This type of attack allows a node to short-cut the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two malicious nodes. Figure 3 describes the redirection of packets with modification attack.

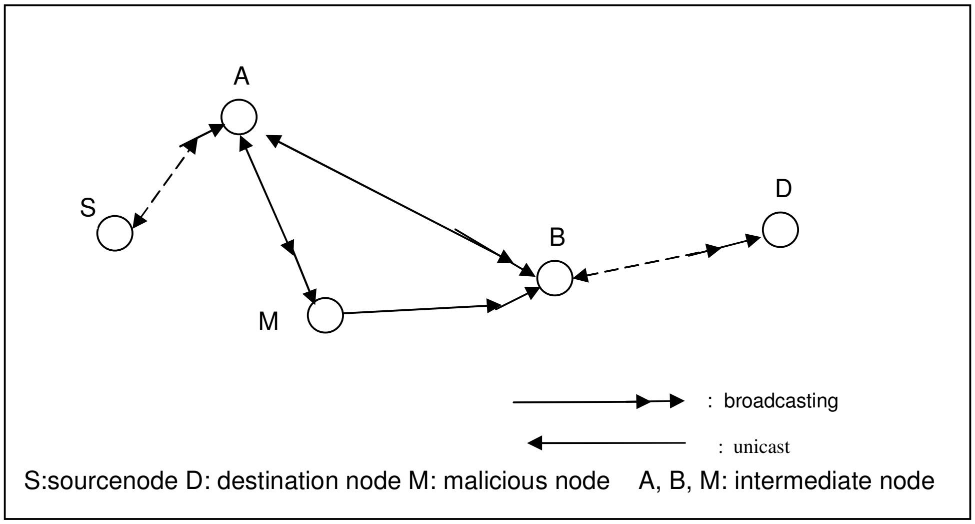
A
S
D
B
M
: broadcasting
: unicast
S:sourcenode D: destination node M: malicious node A, B, M: intermediate node

Figure 3. Redirection of packets with modification attack

2.2. Attack using Fabrication

Conventional routing protocols are difficult to identify whether routing messages they received are legitimate, so the messages fabricated by another node cannot be detected. The rushing attack [13] is a typical example of malicious attacks using fabrication. This attack is carried out against on-demand routing protocols that hold back duplicate messages at every node. An attacker can spread routing messages all through the network, suppressing legitimate routing messages when nodes discard them as duplicate copies. The typical fabrication attack includes: fabricating routing error messages in both AODV and DSR assert that a neighbor can no longer be contacted and broadcast spoofed packets in DSR to poison route caches.

2.3. Attack using Impersonation

A malicious node can initiate many attacks in a network by masquerading as another mode (spoofing). With spoofing, a malicious node can launch many attacks under this environment by misrepresenting its identity as another node to filch unauthorized resource or combined with modification attacks. As an example, a spoofing attack allows the creation of loops in the routing information collected by a node, with the result of partitioning the network.

2.4. Denial-Of-Service Attack

A DoS attack is characterized by an explicit attempt to prevent legitimate users of a service from using that service. A DoS attack on an Internet service application can be achieved by consumption of scarce, limited, or non-renewable resources on which the application (or access to the application) depends. These resources may include network bandwidth, server memory, disk space, CPU time, and access to other computers and networks. Depletion of these resources can prevent the application from functioning or disconnect the application from the Internet, thereby causing service disruption and, thus, making the application unavailable to its users.

2.5. Sybil Attack

The Sybil attack refers to represent multiple identities for malicious intent [14]. This can be achieved if the malicious nodes collude and share their secret keys. As illustrated in Figure 4, A is connected with B, C and the malicious node, M_1. If M_1 represents other nodes M_2, M_3 and M_4 (e.g. by using their secret keys), this makes A believe it has 6 neighbors instead of 3.

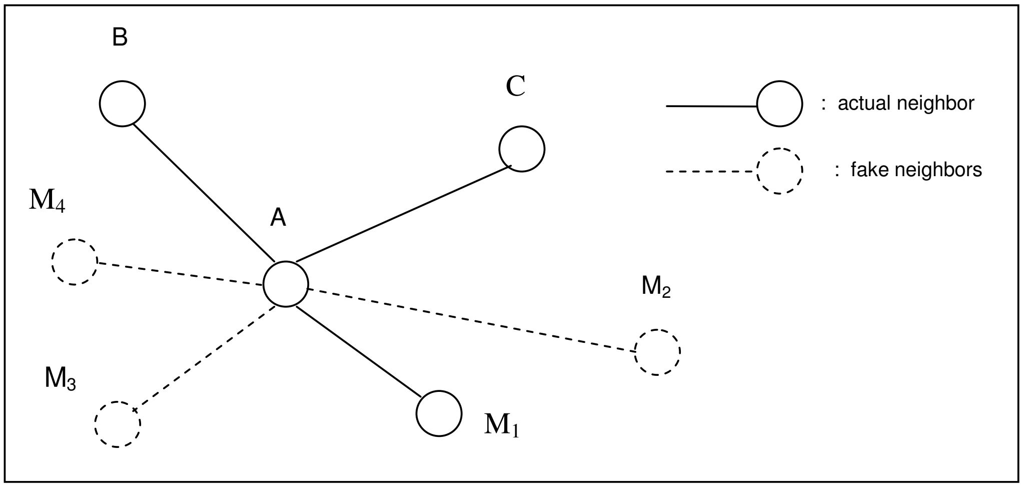

Figure 4. Sybil attack scenario

2.6. Invisible Node Attack

The attack occurs when an intermediate node M does not append its IP address to the route record field of the SRP header. In SRP, the destination node D uses the accumulated route record to establish a path between the source node S and itself. The result of the attack is that M becomes "invisible" in the path and S erroneously believes a path exists between D and itself that does not depend on M. If M leaves the mobile ad hoc network, any route maintenance technique will be unable to notify S that the route is no longer intact because M is "invisible" and it is believed the path does not rely in the existence of M. Table 2 summarizes the different types of attacks, their description and results.

Table 2. Different types of attacks on mobile ad hoc network routing

Type of attacks	Description	Results
Modification	Modify the routing message	DoS, take control of the route
Fabrication	Generate false routing messages	DoS, take control of the route
Wormhole attack	Colluding, take advantage of "tunnels"	Take control of the route
DoS attack	Floods irrelevant data, resource consuming	DoS
Invisible node attack	Malicious node becomes "invisible"	DoS
Sybil attack	Colluding, forging of multiple identities	DoS, take control of the route
Rushing attack	Rushing routing message	Take control of the route

3. RELATED WORK

Security has become a primary concern in MANETs. The characteristics of MANETs pose both challenges and opportunities in achieving security goals. We briefly outline some of the most relevant characteristics of various proposed secure routing protocols in MANET to prevent route discovery process.

Authenticated Routing for Ad-hoc Networks (ARAN) [17] secure routing protocol is an on-demand routing protocol that detects and protects against malicious actions carried out by third-parties and peers in the ad-hoc environment. ARAN provides authentication and non-repudiation services. When a node generates a routing message, it must also sign and every intermediate node verifies the signatures of the source and the previous node, removes the latter, and signs the original message.

Security-Aware ad-hoc Routing (SAR) [18] introduces the idea of trust level as one of the metrics in path finding. Nodes are associated with security levels and every level owns a different key. Only nodes that share a level key can process and forward messages in a specific level.

ARIADNE [19] is an on-demand secure ad-hoc routing protocol that withstands node compromise and relies only on highly efficient symmetric cryptography. ARIADNE guarantees that the target node of a route discovery process can authenticate the initiator, that the initiator can authenticate each intermediate node on the path to the destination present in the node list in the RREQ or RREP messages.

Secure Routing Protocol (SRP) [20] requires that for every route discovery the source and the destination have a security association (SA) between them, which is used to calculate MAC codes to support data integrity and authenticity of route packets.

Secure Ad hoc On Demand distance Vector (SAODV) [21] [22] protocol is an extension of the AODV protocol. The SAODV scheme is based on the assumption that each node possesses certified public keys of all network nodes.

Secure Route Discovery Protocol (SRDP) [23] introduces backward authentication to lighten the security overhead of the protocol. Route integrity, protected via aggregated MACs or multisignatures, is verified in the response messages, not in the broadcast discovery phase.

4. AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. AODV is a hop by hop routing protocols developed for wireless ad-hoc networks [15]. It offers quick adaptation to dynamic link conditions, low processing and memory overhead. When a host wants to find a route to a destination it broadcast a route request (RREQ) message. The RREQ contains addresses (source and destination), sequence number and a broadcast identifier. Nodes other than destination receiving RREQ message either re-broadcast or respond with route reply (RREP), depending on flags setting in RREQ message. When forwarding a RREQ node stores broadcast identifier, source address and maintains a reverse route. In order to avoid loop, RREQ are re broadcasted only when a request with the same source address and broadcast identifier has not been processed before. Concept of sequence number is used for route updation. Thus an intermediate host replies with a RREP when it has a fresh enough route to the destination. Figure 5. shows a typical example of route discovery using AODV protocol. RREQ message was broadcasted by source node. Intermediate node creates and maintains a reverse route to the source node. Destination node, on receiving RREQ sends a unicast RREP to the source node on the same path that was created during RREQ. The incoming RREPs from the source node are processed for consideration is shown in Figure 5. After a source node receives a RREP message, it calls ReceiveReply(Packet P) method - one of the crucial function of AODV. The manner in which the RREP control message is handled is illustrated in the pseudocode of the ReceiveReply(Packet P) function of AODV in Figure 6.

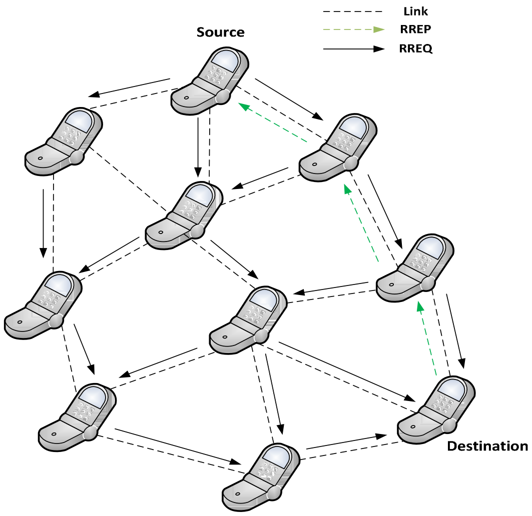

Figure 5. AODV Route Discovery

For every RREP control message received, the source node would first check whether it has an entry for the destination in the route table or not. If it finds one, the source node would check whether the destination sequence number in the incoming control message is higher than one it sent last in the RREQ or not. If the destination sequence number is higher, the source node will update its routing table with the new RREP control message; otherwise the RREP control message will be discarded. In Route Maintenance phase, if a node finds a link break or failure, then it sends RERR message to all the nodes that uses the route.

4.1. Blackhole Attack on AODV Routing Protocol

Blackhole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a false RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbour to the actual destination node. In such a case, the source node would forward all of its data packets to the malicious node, which originally were intended for the genuine destination. The malicious node, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other [16]. Since AODV treats RREP messages having higher value of destination sequence number to be fresher, the malicious node will always send the RREP having the highest possible value of destination sequence number. Such RREP message, when received by source node is treated afresh, too. The fallout is that there is a high probability of a malicious node attempting to orchestrate the blackhole attacks in AODV.

```
AODV: At source node
ReceiveReply (Packet P)
{
     if(P has an entry in Route Table)
      {
         Select Dest_SeqNo from routing table
         If(P_Dest_seqNo > Dest_seqNo)
          {
           Update entry of P in routing table
 Unicast data packets to the route as in RREP
         }
     else
           {
              Discard RREP
           }
        }
else
{
   if(P_Dest_seqNo >= Src_seqNo)
    {
        Make entry of P in routing table
    }
else
      {
        Discard this RREP
    }
  }
}
```

Figure 6. Pseudocode for RecieveReply

5. COUNTERMEASURE TO MITIGATE BLACKHOLE ATTACKS

The solution that we propose here is designed to prevent any alterations in the default operations of either the intermediate nodes or that of the destination nodes. The approach we follow, basically only modifies the working of the source node, using an additional function Pre_ReceiveReply(Packet P). The pseudocode of the same is shown in Figure 6. Apart from this, we also added a new table Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a variable Mali_node to the data structures in the default AODV protocol, as explained further.

In the original AODV protocol, by default, the source node accepts the first fresh enough RREP request coming to it. As compared, in our approach, we store all the RREPs in the newly created table viz. Cmg_RREP_Tab until the time, MOS_WAIT_TIME. Based on the heuristics, we initialize MOS_WAIT_TIME to be half the value of RREP_WAIT_TIME – the time for which source node waits for RREP control messages before regenerating RREQ. In our solution, the source node after receiving first RREP control message waits for MOS_WAIT_TIME. For this time, the source node will save all the coming RREP control messages in Cmg_RREP_Tab table.

Subsequently, the source node analyses all the stored RREPs from Cmg_RREP_Tab table, and discard the RREP having presumably very high destination sequence number. As before, the node that sent this RREP is suspected to be the malicious node. Once, such malicious node is identified, our solution selects a reply having highest destination sequence number from Cmg_RREP_Tab table. It does so, by calling our own method viz. the Pre_ReceiveReply() method. Figure 7 illustrates proposed solution maintains the identity of the malicious node as Malic_node, so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table for that node is not maintained. In addition, the control messages from the malicious node, too, are not forwarded in the network. Moreover, in order to maintain freshness, the Cmg_RREP_Tab is flushed once an RREP is chosen from it. This is testified by the call to the default ADOV routine ReceiveReply(Packet p).

```
Modified AODV: At source node
Pre_ReceiveReply (Packet P)
{
   t0=get(CUR_TIME)
   t1= t0+MOS_WAIT_TIME
  while (CUR_TIME <=t1)
      {
         Store P.Dest_seqNo and P.Node_Id in
Cmg_RREP_Tab table
       }
     While (Cmg_RREP_Tab Is not empty)
         {
          Select Dest_seqNo from Table
   if(Dest_seqNo >= Src_seqNo)
    {
       Malic_Node=Node_Id
       Discard entry from the table
    }
   }
  Select Packet Q for Node_Id having highest
value of Dest_seqNo
ReceiveReply (Packet Q)

}
```

Figure 7. Pseudocode for our Proposed Solution

6. PRELIMINARY RESULTS

For the simulations, we use NS-2 (v-2.33) network simulator. NS-2 provides faithful implementations of the different network protocols. We investigate the performance of our proposed solution with AODV. Performance comparison is done by increasing the number of users. We have implemented our protocol and observe its performance on same topology (same parameters). All nodes are uniformly placed at a distance from each other. Simulation time was 300 seconds. Topology information is communicated to all nodes in 4.06 seconds for 50 nodes. Traffic is generated at 5 second. Statistics are collected every time when number of communicating nodes is increased.

6.1. End-End Delay

The average time to send data from source to destination is calculated for both protocols. Once all the nodes have topology information, average End to End delay is low as compared to AODV. For both protocol the average delay is less than 0.5 seconds. In our proposed solution the increase in delay as compared to number of node is more moderate. AODV send more broadcast (RREQ) for discovering route with increasing number of users. Figure 8 shows the performance results of end-end delay.

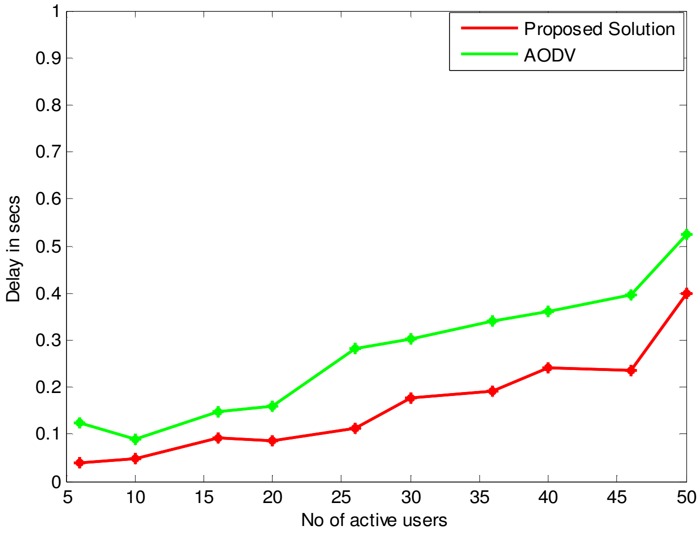

Figure 8. End-End Delay Comparison

6.2. Routing Overhead

Routing Overheads are calculated for AODV and proposed solution. Figure 9 shows the performance results of routing overhead. Since the proposed solution has constant control overhead so it has less routing overhead as the number of user become larger. On the other routing overheads for AODV are much larger then proposed solution. The routing overhead for proposed solution are nearly 10% for 50 active users. Under the same condition the routing overhead for AODV are 27%.

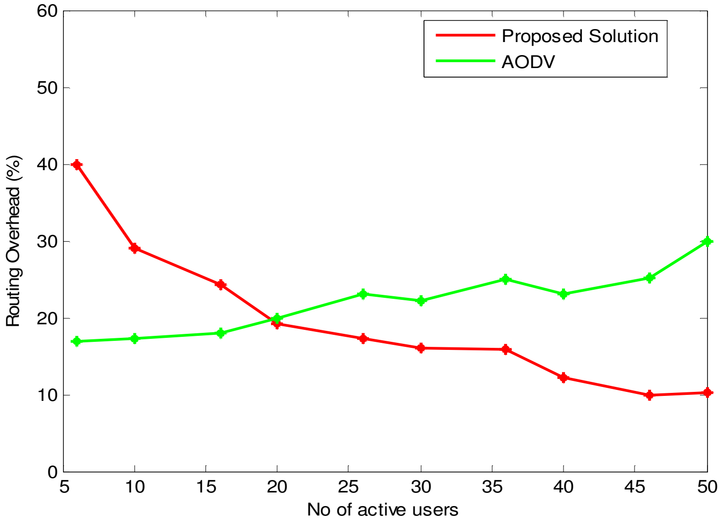

Figure 9. Routing Overhead Comparison

7. Conclusions

With the fact that the default AODV protocol is susceptible to the blackhole attacks, in this research exercise, we attempt at investigating the existing solutions for their viability. Having justified a need for further improvements, we propose an algorithm to counter the blackhole attack on the routing protocols in MANETs. We successfully analyze and demonstrate that with trivial additional overhead in terms of a newMOS_WAIT_TIMEvariableandanew Cmg_RREP_Tab table, we are able to counter the blackhole attacks on the AODV protocol. From the experimental results, we conclude that the proposed solution achieves a very good rise in PDR with acceptable rise in end-to-end delay. Moreover, the proposed algorithm does not entail any hidden overhead on either the intermediate nodes or the destination nodes. Thus, as compared to the other approaches discussed, we believe the proposed algorithm is simple and efficient in implementation. We also emphasize that though the proposed algorithm is implemented and simulated for the AODV routing algorithm, it can also be further trivially extended for use by any other routing algorithms, as well. As part of our future endeavour, we aim to study the impact of varying pause time on the protocol efficiency. In addition, we would also attempt to investigate the impact of varying network size and node mobility on Normalized Routing Overhead in the protocol.

Acknowledgements

The authors would like to thank the support given by G. Pulla Reddy Engineering College and Rayalaseema University for providing various resources in preparing this paper.

References

[1] Marco Conti, Body. *“Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks”*, (Chapter 1), CRC Press LLC, 2003.

[2] C.E. Perkins, E.M. Royer. *“Ad Hoc On-Demand Distance Vector Routing”,* IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, 1999.

[3] D.B. Johnson and D.A. Maltz. *“Dynamic Source Routing in Ad Hoc Wireless Networks”,* in *Mobile Computing*. Academic Publishers, 1996, pp. 153-181.

[4] C.E. Perkins and P.Bhagwat. "*Highly dynamic destination Sequenced Distance-Vector Mobile Computing Systems and Applications*", pp. 90-100, 1999.

[5] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "*Optimized Link State Routing Protocol for Ad Hoc Networks*", in Proc. IEEE International Multi Topic Conference, INMIC 2001. Lahore, 28-30 December 2001, pp. 62-68.

[6] Ebrahim Mohamad, , Louis Dargin. *"Routing Protocols Security In Ad Hoc Networks",* a thesis at Oakland University School of Computer Science Engineering.

[7] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and Herbert Rubens, "*An On-Demand Secure Routing Protocol Resilent to Byzantine Failures*", In ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, September 28, 2002.

[8] Pietro Michiardi and Refik Molva, "*Ad hoc networks security*", In ST Journal of System Research, Volume 4, March 2003.

[9] Pietro Michiardi and Refik Molva **, "***Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks*" **,** European Wireless Conference**,** 2002.

[10] L.Zhou and Z. hass, "*Securing ad hoc networks*", IEEE Network. 13(6): pp. 24-30, November/December 1999.

[11] Benamar KADRI, Mohammed FEHAM, Abdallah M'HAMED, "*A new management scheme of cluster based PKI for ad hoc networks using multi-signature*", In proceeding of the international IEEE Global Information Infrastructure Symposium, Marrakeche, Morocco, pp 167-172, July 2007.

[12] The Network simulator ns-2. Project web page available at at http://www.isi.edu/nsnam/ns/

[13] Hu, Y-C., Perrig, A., and Johnson, D.B., "*Rushing attacks and defense in wireless ad hoc network routing protocols*", Proc. Of the ACM Workshop on Wireless Security (WiSe '03), pp. 30-40, 2003.

[14] John Rittinghouse, James Ransome, "*Wireless operational security"*, Digital Press, 2004.

[15] Perkins, C., Belding-Royer, E., and Das, S., "*Ad hoc On-Demand Distance Vector (AODV) Routing*", RCF 3561. 2003, Internet Engineering Task Force.

[16] Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "*Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method.*" In: International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007.

[17] B.Dahill, B.N. Levine, E. Royer and C.Shields, "*ARAN: Asecure Routing Protocol for Ad Hoc Networks*", UMass Tech Report 02-32, 2002.

[18] S. Yi, P. Naldurg and R. Kravets, "*Security-aware ad hoc routing for wireless networks*", In MobiHOC, October 2001.

[19] Y –C. Hu, A. Perrig, and D.B. Johnson, "*Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks*", In Proc. 8th ACM International Conference Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, PP. 12-23.

[20] P. Papadimitratos and Z. Haas, "*Secure routing for mobile ad hoc networks*", In Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS), 2002.

[21] M. Zapata, "*Secure Ad hoc On-demand Distance Vector (SAODV)",* Internet Draft, draft-guerrero-manet-saodv-01.txt, 2002.

[22] Zapata, M. G., "*Secure ad-hoc on-demand distance vector (SAODV) routing",* IETF MANET, internet draft (Work in progress), draft-guerrero-manet-saodv-00.txt, 2001.

[23] J. Kim and G. Tsudik., "*Srdp: Securing route discovery in dsr*", In MobiQuitous. PP. 247-260, IEEE Computer Society 2005.

Authors

Sreedhar.C received B.E (CSE) and M.E (CSE) degree in 2000 and 2007, respectively. Presently pursuing Doctorate Degree (Ph.D) in Computer Science & Engineering from Rayalaseema University, Kurnool and working as Associate Professor in CSE Department in G. Pulla Reddy Engineering College, Kurnool. His research interest includes Wireless networks, Security, Routing Protocols. He has published two International Journals and attended one International conference.

Dr. S. Madhusudhana Verma has received M.Sc in 1986, M.Phil in 1998 and Ph.D in 1994 from Sri Venkateswara University, Tirupathi. He is working as Professor and Head of OR&SQC at Rayalaseema University, Kurnool. His research interests are Reliability Engineering, Statistical modelling and Computer Science. He attended 13 National/International Conferences and published 14 research articles in National/International Journals and guided Doctoral and M.Phl Degrees.

Dr. N. Kasiviswanath has completed B.E in CSE from Marthwada University, M.S from BITS, Pilani and Doctorate Degree (Ph.D) from Rayalaseema University. He has 19 years of teaching experience. He has published 20 research papers in National/International Journals/Conferences. Presently he is working as Professor & HOD CSE Department, G. Pulla Reddy Engineering College, Kurnool.