Asian Journal of Information Technology 13 (2): 68-76, 2014
ISSN: 1682-3915

Performance Improvement of Security Attacks in Wireless Mobile Ad Hoc Networks

N. Kirubakaran and A. Kathirvel
Faculty of Information Technology,
Vivekanandha College of Engineering for Women, Tamilnadu, India

Abstract: Mobile Ad hoc Networks (MANET) are self-creating, self-administering and self-organizing entities. Thus, a set of self-motivated mobile wireless users is able to dynamically exchange data among themselves even in the absence of a predetermined infrastructure and controller. In this study, researchers extended a solution Enhanced Triple Umpiring System (ETUS) to generic attack such as Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Gray hole attack, Jelly fish attacks, Network jamming signal, Masquerading data attack, Man in the middle attack, Replay attack, Rushing attack, Sybil attack, Selfish node attack, Sink hole attack and Worm hole attack extensive simulation studies using QualNet 5.0 establish the soundness of the proposal.

Key words: MANET, ETUS, attacks and security, sink, worm

INTRODUCTION

Mobile Ad hoc Networks (MANET) are self-creating, self-administering and self-organizing entities. Thus, a set of self-motivated mobile wireless users is able to dynamically exchange data among themselves even in the absence of a predetermined infrastructure and controller. Each user of mobile ad hoc network also acts as a router allowing other users to communicate through their mobile communication device. The communication range of each device is limited, therefore at any given time a user can exchange packets only with any one of the devices in its transmitting or receiving range.

Unlike the conventional cellular networks that rely on extensive infrastructure to support mobility, a MANET does not need expensive base stations and wired infrastructure. These features are important for potential use in a wide variety of disparate situations. Such situations include battlefield communications and disposable sensors which are dropped from high altitudes and are dispersed on the ground for hazardous materials detection. Civilian applications include emergency situations such as responses to hurricane, tsunami, earthquake and terrorism. Another interesting example is the case, where a set of mobile vehicles on the highway form an ad hoc network of their own in order to provide vehicular traffic management. Security provisioning in wireless ad hoc networks plays an integral part in determining the success of network centric warfare as envisioned for future military operations (Kathirvel and Srinivasan, 2011a, b; Georgiadis *et al*., 2006; Raj and Swadas, 2009). Thus, security is an important issue for these mission-critical applications (Rai *et al*., 2010).

The unique characteristics of Wireless Mobile Ad Hoc Networks Routing algorithms result in new sets of wireless mobile computing attacks. The majority of these attacks are directed at the algorithmic capabilities; the means of communicating routing message and the data forwarding packet. The list of wireless mobile ad hoc network attacks as follows: Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Gray hole attack, Jelly fish attacks, Network jamming signal, Masquerading data attack, Man in the middle attack, Replay attack, Rushing attack, Sybil attack, Selfish node attack, Sink hole attack and Worm hole attack. Each attack is explained in study 2.

This study is based on the foundations of a two system already proposed us, Self_USS and ETUS (Kathirvel and Srinivasan, 2011a, b).

Kathirvel and Srinivasan (2011a) have proposed a self umpiring system for security in mobile ad hoc network. In the self-umpiring system each node is issued with a token at the inception. The token consists of two fields: NodeID and status (Kathirvel and Srinivasan, 2011a, b). NodeID is assumed to be unique and deemed to be beyond

Corresponding Author: N. Kirubakaran, Faculty of Information Technology, Vivekanandha College of Engineering for Women, Tamilnadu, India

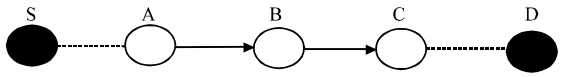

Fig. 1: Self umpiring system model; S: Source; D: Destination; A, B, C: Intermediate nodes. During data forwarding, A: The umpire for B: During route RREP, C: The umpire for B

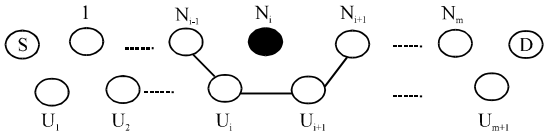

Fig. 2: Enhanced triple umpiring system model; N_{i-1}, N_i, N_{i+1}, ..., N_m intermediate nodes in the active path. U_i, U_{i+1}, ..., U_{m+1} = Corresponding umpires. For node N_{i-1}, U_i, U_{i+1} in the forward path and N_{i+1}, U_i, U_{i+1} in the reverse path. Assume that node N_i becomes culprit node in the packet forwarding operation. ETUS form an new route using umpiring nodes. Node N_{i-1}, U_i and U_{i+1} used to form an alternative path to reach node N_{i+1}. In the alternative path, their is no independent umpires are used (i.e.) self-umpire. Self-umpire nodes have dual roles packet forwarding and umpiring

manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node which confers it the freedom to participate in all network activities. Each node in order to participate in any network activity, say, route request RREQ has to announce it's token. If it's status bit is "1" indicating "red flag" protocol does not allow the node to participate in any network activity. The working of the self-umpiring system is explained with reference to Fig. 1.

In the self-umpiring system all the nodes have dual roles packet forwarding and umpiring. In the forward path during data forwarding, each node monitors the performance of immediate next node. That way, node A can tell correctly whether B is forwarding the packet sent by it by promiscuously hearing B's transmissions. Similarly during reply process RREP, C can verify whether B is unicasting the route reply RREP and whether the hop count given by B is correct. Thus, during forward path A is the umpire for B and C is the umpire for B during reverse path operations. When a node is found to be misbehaving say dropping data packets, the corresponding umpire immediately changes the status bit of guilty node to "1" indicating red flag.

Enhanced Triple Umpiring System (ETUS) Model (Kathirvel and Srinivasan, 2011a, b) is presented in Fig. 2.

The active path is specified by nodes source, node 1, ..., node N_{i-1}, node N_i, ..., node N_m and the destination node. Thus, there are N_{m+2} nodes in the active path U_1, U_2, ..., U_i, U_{i+1}, ..., U_m and U_{m+1} are umpiring nodes. Umpire U_i is situated in the communication zones of nodes N_i, N_{i-1}, U_{i-1} and U_{i+1}. For node N_i the two umpires will be U_i and U_{i+1}. The third umpire will be N_{i-1} is the forward path and N_{i+1} in their reverse path. Thus, when N_i is found to be misbehaving say dropping packets or changing Hop count or sequence number, umpire nodes U_i, U_{i+1} and N_{i-1} in the forward path and N_{i+1} in the reverse path sends a M-ERROR message to the source and sets the status bit of guilty node N_i to "1" indicating red flag by M-Flag message.

LITEARTURE REVIEW

The Key Distribution Center (KDC) architecture is the main stream in wired network because KDC has so many merits: efficient key management including key generation, storage and distribution and updating. The lack of Trusted Third Party (TTPs) key management scheme is a big problem in ad hoc network (Kathirvel and Srinivasan, 2011a, b).

Different types of attacks on MANET were discussed by Rai *et al.* (2010) they have design a security mechanism by which they can minimize or completely remove many of those attacks.

Soldo *et al.* (2011), to gave solution for blacklisting attacks, in these study they study the problem of forecasting attack sources based on past attack logs from several contributors. They formulate this problem as an implicit recommendation system.

Rani and Sekhar (2012) propose a detection and prevention of wormhole attack in stateless multicasting. Their scheme has no central administrator. They have shown that their schemes can wormhole attacks.

Georgiadis *et al.* (2006) make a survey of threats and possible solutions for resource allocation and cross layer control in wireless networks. Raj and Swadas (2009) propose a solution for black hole attacks. It was implemented in prominent AODV protocol based MANET. Tsou *et al.* (2011) developing a novel scheme BDSR to Avoid Black Hole Attack Based on Proactive and Reactive Architecture. Yu *et al.* (2007) proposed an solution of a distributed and cooperative black hole node detection and elimination mechanism.

Jyoshna and Prasad (2012) propose a solution for Byzantine Attacks in Ad Hoc Networks using SMT protocol provides a way to secure message transmission by dispersing the message among several paths with minimal redundancy. Megha and Jain (2011) gave an

solution for Gray hole attack. They use an Intrusion Detection System (IDS) to monitors the network or system activities for malicious activities or policy violation and produces reports to a management station. It takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighbors nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again and Broadcasting Route Request (RREQ) messages.

A mechanism to develop an algorithm that detects the jellyfish attacks at a single node and that can be effectively deployed at all other nodes in the ad hoc network (Jayasingh and Swathi, 2010). They gave a solution that detects the Jellyfish reorder attack based on the reorder density which is a basis for developing a metric.

This study focuses on jamming at the Transport/ Network layer (Timothy, 2010). Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing and sequence is available to the attacker for sensing.

All the above schemes only try to protect the system from the attacker but not bother about quarantining attackers. The ETUS Systems (Kathirvel and Srinivasan, 2011a, b) not only detect the mischievous nodes but also prevent their further participation in the network.

MODELS AND ASSUMPTIONS

In this study, researchers formulate the Wireless Mobile Ad hoc Network Model and security model and then describe the security attacks.

Network Model: Researchers consider a wireless mobile ad hoc network consisting of an unhindered number of networking nodes. For differentiation purpose, researchers require each node to have a unique non zero ID. Assumptions made in the design of triple umpiring system are as follows:

- A wireless mobile ad hoc network where nodes are free to move about or remain at stand still, at their will is assumed. Each node may join to the network or node may leave from the network at any time
- The source and the destination node are not malicious
- Nodes may fail at any time
- Every node in the network have neighbors list
- There exists a bi-directional communication link between any pair of nodes which is a requirement for most wireless MAC layer protocols including IEEE 802.11 for reliable transmission
- Wireless interfaces support promiscuous mode of operation. Most of the existing IEEE 802.11 based wireless cards support such promiscuous mode of operations to improve routing protocol performance

The promiscuous mode may also find additional communication overhead and energy utilization in order to process the transit packets. Researchers do not address the energy efficiency in this research.

Security model: Mobile ad hoc networks are vulnerable to security attacks due to its features of shared radio channel, insecure open medium, dynamic changing topology, lack of cooperative algorithms, lack of centralized monitoring, limited resource availability and physical vulnerability. Attacks on MANET can be classified into two categories, namely, passive attacks and active attacks. A passive attack does not disrupt the operation of the network. The passive attackers are less vulnerable to the network security. Researchers do not address passive attackers who eavesdrop and record the wireless transmissions. An active attack attempts to destroy or alter the data packets and routing messages being exchanged in the network. The active attackers are more vulnerability to security attacks. In this study, researchers address only active attackers.

The unique characteristics of wireless mobile ad hoc networks routing algorithms result in new sets of wireless mobile computing attacks. A partial listing of mobile ad hoc network are brief look at them is in order: Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Gray hole attack, Jelly fish attacks, Network jamming signal, Masquerading data attack, Man in the middle attack, Replay attack, Rushing attack, Sybil attack, Selfish node attack, Sink hole attack and Worm hole attack.

Black listing attack: In this attack, a malicious node falsely advertises good node is behaving maliciously. It is trick a network into believing a good node is behaving maliciously.

Black hole attack: During route discovery processes, a malicious node falsely advertises good path with smaller hop count (Yu *et al*., 2007). It causes complete refusal to participate in a network.

Byzantine attack: In this attack, a set of compromised intermediate nodes which creates the collusion. The collusion includes selectively dropping the packets, set of compromised nodes creating routing loops and routing packets on less stable path. It is hard to detect.

Changing route tables' attack: In this type of attack, an adversary node changing the routing tables may result in overflow of the routing tables, sub-optimal routing and congestion in portions of the network or even make some parts of the network inaccessible.

Gray hole attack: In this attack, a malicious node or a set of compromised nodes which can selectively dropping the data packets (Tsou *et al*., 2011). It is similar to the byzantine attack. Gray hole attack is difficult to detect.

Jelly fish attack: In the Jelly fish attack, an adversary node change or modify genuine end to end delay and jitter values. End to end delay and jitter is the most important parameter for Quality of Service (QoS). Hence, the performance level of a service offered by the network to the user is degraded.

Network jamming signal: In this form of attack, the malicious node initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. It then transmits signals on that frequency so that error free reception at the receiver is hindered.

Masquerading data attack: In this attack, the adversary node may inject unwanted data into the network which causes routing loop and spoofing.

Man in the middle attack: It is a class of attack, an intermediate node maliciously manipulates the routing messages creating loops, wormhole and biasing the network to route the packets through the malicious nodes.

Replay attack: A breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction. It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerading data attack.

Rushing attack: In this attack, a node rushes a corrupt data packet identified to match the real packet. The receiving node first accepts the corrupt data packet, dropping it and then, on receipt of the good data packet matches the packet identity to that of the prior and drops it.

Sybil attack: A Sybil attack is one in which an attacker subverts the reputation system of a peer to peer network by creating a large number of pseudonymous entities using them to gain a disproportionately large influence. It is hard to detect.

Selfish node attack : A selfish node attack is one in which an attacker that refuse to fully participate in the network routing operations.

Sink hole attack: In this attack, adversary node taking on more routing that needed, forcing data packet pass through itself becoming an overly critical network node.

Worm hole attack: Two attackers collude to achieve a wormhole (Rani and Sekhar, 2012). When an attacker receives packets, it sends them to the other through the wormhole and then it replays them into the network.

UMPIRING SYSTEM SECURITY MODELS: SELF_USS AND ETUS

In the self-umpiring system each node is issued with a token at the inception. The token consists of two fields: NodeID and status. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node which confers it the freedom to participate in all network activities. Each node in order to participate in any network activity, say Route Request RREQ has to announce its token. If status bit is "1" indicating "red flag" protocol does not allow the node to participate in any network activity. The working of the self-umpiring system is explained with reference to Fig. 1.

In the self-umpiring system all the nodes have dual roles-packet forwarding and umpiring. In the forward path during data forwarding each node monitors the performance of immediate next node. That way, node A can tell correctly whether B is forwarding the packet sent by it by promiscuously hearing B's transmissions. Similarly during reply process RREP, C can verify whether B is unicasting the route reply RREP and whether the hop count given by B is correct. Thus, during forward path A is the umpire for B and C is the umpire for B during reverse path operations.

When a node is found to be misbehaving say dropping packets, the corresponding umpire immediately sends a M-ERROR message to the source and the status bit of guilty node is set to "1" red flag using M-Flag message. In order to correctly correlate the overheard messages an additional field next-hop has been introduced in all routing messages as done in SCAN (Kathirvel and Srinivasan, 2011b). Though there are several kinds of misbehavior that could be captured by promiscuous hearing we are focusing only on two types of malicious actions: dropping packets and transmitting false hop count.

The token system is similar to the one adopted by SCAN. In SCAN token is issued by a set of neighbors; minimum k neighbors are required to sign tokens; asymmetric cryptography has been adopted to prevent forgery of tokens. Further tokens are to be renewed at periodic intervals. In the system there is no change in the token it can be used for the full lifetime of the node, if the node continuously behaves correctly. At the instance of the first offence the status of the guilty node is set to 1 preventing its further participation in the network.

Researchers assume that no node can alter its own status bit. Only the designated umpire corresponding to the forward or reverse path under consideration can change the status bit. For example the status bit of B in Fig. 2 can be changed only by A in the forward path and only by C in the reverse path. It is also assumed that a node cannot announce wrongly its token particulars NodeID and status bit.

In this study, researchers consider an attacker who can perform any combination of attacks that are within the above generic attacks such as Black hole attack, Jelly fish attack, Man in the middle attack, Selfish node attack, Sink hole attack and Worm Hole Attack Model.

The aim is designing the security system is to limit the overhead to as minimum as possible while getting a good improvement in throughput. SCAN System with minimum k neighbors signing, encryption, periodic renewal of tokens is definitely robust but at a huge cost of control overhead and energy efficiency.

In the Triple Umpiring System each node is issued with a token at the inception. The token consists of two fields: NodeID and status. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node which confers it the freedom to participate in all network activities. It is assumed that any node can not change its own status bit. Only designated umpires can change the status bit of the specified node under their observation.

Each node in order to participate in any network activity, say Route Request RREQ has to announce it's token. If status bit is "1" indicating "red flag" protocol does not allow the node to participate in any network activity.

Enhanced Triple Umpiring System (ETUS) Model is presented in Fig. 2. The active path is specified by nodes source, node 1, ..., node N_{i-1}, node N_i,..., node N_m and the destination node. Thus, there are N_{m+2} nodes in the active path U_1, U_2, ..., U_i, U_{i+1}, ..., U_m and U_{m+1} are umpiring nodes. Umpire U_i is situated in the communication zones of nodes N_i, N_{i-1}, U_{i-1} and U_{i+1}. For node N_i the two umpires will be U_i and U_{i+1}. The third umpire will be N_{i-1} is the forward path and N_{i+1} in their reverse path. Thus, when N_i is found to be misbehaving say dropping packets or changing Hop-count or sequence number, umpire nodes U_i, U_{i+1} and N_{i-1} in the forward path and N_{i+1} in the reverse path sends a M-ERROR message to the source and sets the status bit of guilty node N_i to "1" indicating red flag by M-Flag message.

Since, N_i has been prevented from participation the active path is cut. An alternative path is established via N_{i-1}, U_i, U_{i+1} and N_{i+1}. Since, the concerned nodes have already the required information, they seamlessly switch over to alternative route. The segment N_{i-1}, U_i, U_{i+1} and N_{i+1} will be working under self umpiring system mode already proposed by us (Kathirvel and Srinivasan, 2011a). This means N_{i-1} will play the role of umpire for U_i, U_i for U_{i+1} and U_{i+1} and N_{i+1}. For the rest of the segments, ETUS will operational. In the ETUS, researchers introduced the following attacks it includes Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Gray hole attack, Jelly fish attacks, Network jamming signal, Masquerading data attack, Man in the middle attack, Replay attack, Rushing attack, Sybil attack, Selfish node attack, Sink hole attack and Worm hole attack.

IMPLEMENTATION OF SECURITY ATTACKS IN ETUS

Researchers implement generic security attacks in ETUS on top of traditional AODV protocol but its principal is applicable to other routing protocol as well. Researchers modify the famous AODV routing protocol and add a new field, next-hop, in the routing messages, so that a node can correlate the overheard packets correctly. It is based on three algorithms.

Algorithm 1 describes route request procedure. During route request procedure it check the following list of attacks such as Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Jelly fish attacks, Network jamming signal and Man in the middle attack.

Algorithm 2 deals with route reply procedure. During route reply procedure it check the following list of attacks includes Replay attack, Sybil attack, Selfish node attack, Sink hole attack and Worm hole attack.

Algorithm 3 which involves packet forwarding operation is modified for ETUS implementation. During data packet forwarding procedure it check the following list of attacks includes Gray hole attack, Masquerading data attack and Rushing attack. Each node in order to participate in any network activity, says Route Request (RREQ) has to announce it's token as described in algorithm 1. If the node status bit is "1" indicating red flag protocol does not allow the node to participate in any network activity.

Algorithm 1 (While broadcasting an Generic ETUS_RREQ packet):

```
// This algorithm takes care of broadcast of Generic ETUS_RREQ packets
1:  Assign initial values for bla, bha, bam crta, jfa, njs, mima = 0
2:  for each Generic ETUS_RREQ packet (P) received do
2:    if node status is green flag then
3:      // broadcast RREQ
4:       nodeprevhop ← nodecurrenthop [node address]    // it support
        promiscuous operation
5:      neighhop1← prevhop[node address]                // umpire 1
6:      neighhop2← nexthop[node address]                // umpire 2
7:      repeat the steps from step 2 to step 6 until it destination node is
        reached.
8:  else
9:    increment bla // Black listing attack
10:   increment bha // Black hole attack
11:   increment bam // Byzantine attack
12:   increment crta // Changing route tables attack
13:   increment jfa // Jelly fish attack
14:   increment njs // Network Jamming Signal
15:   increment mima // Man in middle attack
16:   if (bla >1 && bha >1 && bam >1 && crta >1 && jfa >1 &&
      njs >1 && mima >1)
17:     node status change to red flag
17:   drop generic ETUS_RREQ packet (P) received
18:   endif
19: endfor
```

In the triple umpiring system, three umpiring nodes are used to convict the malicious node in packet forwarding operation. The algorithm 2 which takes care of unicast route reply packets is given. In the algorithm 2 the following steps of operation should be taking place are:

- Destination node D should appoint first umpire node. The destination node D forwards its list of neighbors to the previous node
- The previous node has its own list of neighbors. Now previous node finds intersection of destination node and its own list of neighbors
- From among the intersection nodes, it appoints one node as umpire
- The umpire so appointed sends its neighbor list to previous node and its adjacent umpire node
- Researchers find the intersection of neighbors list from the previous node and umpire node. The new intersected list of neighbors as send next previous node

Algorithm 2 (While unicasting an Generic ETUS_RREP packet):

```
// This algorithm takes care of unicast of generic ETUS_RREP packets
1:  Assign initial values for ra, sa, sna, sha, wha = 0
2:  for each generic ETUS_RREP packet (P) received do
3:   if node status is green flag then
4:     // set designated umpires
5:     // Node send its neighbor list to its previous node
6:    for (i = 0; i<m; i++)
7:    for (j = 0; j<n;j++)
8:    if a[i] is equal to b[j]then
9:    c[k] is equal to a[i] // Intersection of neighbor list, umpire is
      appointed
10:    k++
11: end if
12: end for
13: end for
14: neighhop1← prevhop[node address]                  // umpire 1
15: neighhop2← nexthop[node address]                  // umpire 2
16: nodenexthop ←_nodeprevhop [node address]  // it support promiscuous
    operation
17:    // unicast ETUS_RREP to previous node
18:    if node current hopcount and neighhop1 and neighhop2 are equal to
       node next hopcount then process this RREP as specified in the
      standard protocol
19:    repeat the steps from step 2 to step 18 until it source node is reached.
20:   else
21:          increment ra // Reply attack
22:          increment sa  // Sybil attack
23:          increment sna // Selfish node attack
24:          increment sha // Sink hole attack
25:          increment wha // Worm hole attack
26:          if(ra >1 && sa >1 && sna >1 && sha >1 && wha >1)
27:                node status change to red flag
28:     save current RREP message in the buffer
29:       // Misbehaving node is marked as malicious node
30:       // it broadcast MERR packet to 1-hop or 2-hop node distance
31:       node status is marked as red flag
32:       // Salvaging is used to identified new path
33:      currentnode is the source node and the source node becomes a
        destination node thus start
        RREQ_SRR procedure
34:      Process this RREQ_SRR and RREP_SRR as specified in the standard
         protocol
35:      it reaches the RREP_SRR to the currentnode
36:      retrieve previous saved RREP message from the buffer
37:      send RREP message in newly identified path to the source node
38:          process this generic ETUS_RERR message as specified in the
          standard protocol
39:      end if
40:    endif
41:  endfor
```

Algorithm 3 deals with data packets forwarding:

Algorithm 3 (While sending an Generic ETUS_data packet):

```
// This algorithm takes care of Generic ETUS_data packets
Assign initial values for gha, mda, r = 0
for each generic ETUS_DATA packet (P) received do
  if node status is green flag then
    // send a packet to the next forwarded node
    // it tampered with the payload or header of the currently sent packet
    nodenexthop←nodecurrentpacketheader          // it saves current packet header information
    neighhop1←nodecurrentpacketheader            // umpire 1
    neighhop2←nodecurrentpacketheader            // umpire 2
    // it keeps the header information until next packet is forwarded to the node
    // tampered header information is cross checked with umpire nodes
    if node next hop←current packet header and neighhop1← node current packet header and neighhop2←node current packet header is equal to prevhop←current packet header
    Repeat the steps from 2 to step 10 until all packets are delivered
else
        increment gha // Grey hole attack
        increment mda // Masquerading attack
        increment wha // Worm hole attack
        if(ra >1 && sa >1 && sna >1 && sha >1 && wha >1)
            node status change to red flag
    // nodenextnode has dropped the packet thus the malicious node. nodeprevnode, neighhop1 and neighhop2 is umpire node for next immediate node
    // it has marked as malicious node
    it broadcast MERR packet to 1-hop or 2-hop node distance
    node next node (maliciousnode) status is marked as red flag
    // To form a backup path using the umpiring nodes
    Nodeprevnode sent link error message to the source node and immediately stop the packet
        forwarding operation
    // Backup route is formed using nodeprevnode, neighhop1, neighhop2 and malicious next node
    Nodeprevnode.nexthopnode← neighhop1
    Nodeprevnode.neighhop1.nexthopnode← neighhop2 and
        Malicious node.neighhop1←Malicious node.neighhop2
    Malicious node.neighhop2.next hop node← Malicious next node
    // Routing tables of nodeprevnode, neighhop1, neighhop2, malicious next node to be updated.
    // Nodeprevnode, neighhop1, neighhop2 and maliciousnode of Neighhop1 and Neighhop2
        values are set to zero.
    Nodeprevnode set new backup path to source node.
    // source node restart packet forwarding operation and send the packets using backup route.
    // In backup path, they will call self-USS procedure
    CALL SELF-USS_DATA PACKET PROCEDURE
        process this RERR message as specified in the standard protocol
  endif
endif
endfor
```

While sending a Self_USS_data packet

```
for each Self_USS_DATA packet (P) received do
  if node status is green flag then
    // send a packet to the next forwarded node
    // it tampered with the payload or header of the currently sent packet
    node next hop ← node current packet header
    // it saves current packet header information
    // it keeps this header information until next packet is forwarded to the node
    // node next node has dropped the packet thus the malicious node
    if node current packet header is equal to prevhop←current packet header
        Repeat the steps from 2 to step 9 until all packets are delivered
  else // it has marked as malicious node. Broadcast MERR packet to 1-hop or 2-hop node distance
    node next node status is marked as red flag
    // Self_USS node sent link error message to the source node
    // process this RERR message as specified in the standard protocol
  endif
endif
endfor
```

SIMULATIONS AND RESULTS

Researchers use a simulation model based on QualNet 5.0 (Network Simulator) in the evaluation (Kathirvel and Srinivasan, 2011a, b). The performance evaluations are based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a rectangular (1500×600 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11 (Bajaj *et al*., 1999; IEEE, 1999). The performance setting parameters are given in Table 1.

Before the simulation we randomly selected a 30% of the network population as generic malicious behavior nodes. Each flow did not change its source and destination for the lifetime of a simulation run. Researchers had kept the simulation time as 1500 sec, so as to enable us to compare our results with that of ETUS.

Throughput: In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is nothing but a ratio between the numbers of packets received by the destinations to the number of packets sent by the sources.

Researchers present in Table 2 the packet delivery ratios for 30% malicious node with node mobility varying between 0-20 m sec^{-1}.

In the above result there is X, Y and Z variables are used. Variable X indicates 100% attacks detected and whereas Y and Z indicates 50 and 0%, respectively. In general packet delivery ratio decreases as mobility and percentage of malicious nodes increase. As compared to plain AODV and ETUS, generic ETUS results are superior. Researchers offer the comments in the result analysis.

Cmmunication overhead: Communication overhead can be evaluated based on the number of transmissions of

control messages like RREQ, RREP and RERR in the case of plain AODV and in addition M-ERROR, M-Flag, Umpire, Neighbor list messages in the TUS and ETUS (Table 3).

In addition, salvaging concept introduced in ETUS, it uses special control messages like $RREQ_{SRR}$, $RREP_{SRR}$ and $RERR_{SRR}$. RREQ are to be decimated to the entire network where as RREP messages are unicasts.

In the above result there is X, Y and Z variables are used. Variable X indicates >50 control packets are used for the specific purpose and whereas Y and Z indicate in addition to 100 control packets and >100 packets, respectively. As compared to plain AODV and ETUS, generic ETUS results incur additional control packets.

Table 1: Parameters setting

Parameters	Values
Simulation time	1500 sec
Propagation model	Two-ray ground reflection
Transmission on range	250 m
Bandwidth	2 Mbp
Movement model	Random way point
Maximum speed	0-20 m sec^{-1}
Pause time	0 sec
Traffic type	CBR (UDP)
Payload size	512 bytes
Number of flows	10/20

Table 2: Packet delivery ratios for 30% malicious node with node mobility varying between 0-20 m sec^{-1}

	Mobility (m sec^{-1})				
Generic attacks	0	5	10	15	20
Black listing attack	X	X	Y	X	X
Black hole attack	X	Y	Z	Y	X
Byzantine attack	Y	Z	Y	X	X
Altering tables'attack	X	Y	Z	Y	X
Gray hole attack	X	X	Y	X	X
Jelly fish attacks	X	Y	Z	Y	X
Network jamming signal	Y	X	Y	X	Z
Masquerading data attack	X	X	Y	X	X
Man in the middle attack	X	Y	Z	Y	X
Replay attack	Y	Z	Y	X	X
Rushing attack	X	X	Y	X	X
Sybil attack	Z	Z	Z	Z	Y
Selfish node attack	Y	Z	Y	X	X
Sink hole attack	X	Y	Z	Y	X
Worm hole attack	X	Y	Z	Y	X

Analysis of results: Researchers find that Generic ETUS yields much higher packet delivery ratio compared to Self_ USS, Self_USS with SRR, TUS, SCAN, ETUS and plain AODV in the presence of 30% malicious nodes in Table 4.

It is found that with Generic ETUS there is a higher packet delivery ratio ranging from 27.04% (Self_USS, 0 m sec^{-1} mobility) to 28.51% (TUS 20 m sec^{-1} mobility).

Researchers present a comparison of communication overhead for Self_USS, Self_USS with SRR, TUS (Kathirvel and Srinivasan, 2011b), ETUS, generic ETUS and plain AODV in the presence of 30% malicious nodes in Table 5. It is found that with Generic ETUS there is a decrease the communication overhead ranging from 32.90% (Self_USS, 0 m sec^{-1} mobility) to 22.92% (Self_USS, 20 m sec^{-1} mobility).

However, Generic ETUS communication overhead is much higher compared to Self_USS with SRR. For example, with mobility of 20 m sec^{-1}, Generic ETUS communication overhead is 125% as compared to Self_USS with SRR. Researchers are unable to compare communication overheads with SCAN since absolute values are not available. Researchers find that the proposed generic ETUS yield much higher output as compared to all other system.

Tables 3: Communication overhead for 30% malicious node with node mobility varying between 0-20 m sec^{-1}

	Mobility (m sec^{-1})				
Generic attacks	0	5	10	15	20
Black listing attack	X	X	Y	X	X
Black hole attack'	X	Y	Z	Y	X
Byzantine attack	Y	Z	Y	X	X
Altering tables'attack	X	Y	Z	Y	X
Gray hole attack	X	X	Y	X	X
Jelly fish attacks	X	Y	Z	Y	X
Network jamming signal	Y	X	Y	X	Z
Masquerading data attack	X	X	Y	X	X
Man in the middle attack	X	Y	Z	Y	X
Replay attack	Y	Z	Y	X	X
Rushing attack	X	X	Y	X	X
Sybil attack	Z	Z	Z	Z	Y
Selfish node attack	Y	Z	Y	X	X
Sink hole attack	X	Y	Z	Y	X
Worm hole attack	X	Y	Z	Y	X

Table 4: Throughput for Self_USS, Self_USS with SRR, TUS, plain AODV, SCAN, ETUS and generic ETUS

	Throughput for malicious node = 30%						
Mobility (m sec^{-1})	Self_USS	Self_USS with SRR	TUS	SCAN	Plain AODV	ETUS	Generic ETUS
0	76.22	78.18	90.54	90	70.44	94.92	96.83
5	73.04	75.02	86.15	85	45.18	92.32	94.45
10	70.25	72.18	82.99	83	37.89	90.52	92.69
15	69.58	71.49	81.79	81	32.55	86.85	88.88
20	68.46	70.41	80.45	80	32.07	85.78	87.98

Table 5: Communication overhead for Self_USS, Self_USS with SRR, TUS, plain AODV, ETUS and generic ETUS

	Communication overhead for malicious node = 30%					
Mobility ($m\ sec^{-1}$)	Self_USS	Self_USS with SRR	TUS	Plain AODV	ETUS	Generic ETUS
0	15142	14841	23998	14136	21234	20125
5	16010	15711	24978	14603	21366	20436
10	16813	16501	25897	15082	22345	21234
15	17639	17334	26769	15580	22553	21433
20	18372	18071	27874	16082	23984	22584

CONCLUSION

Researchers have conducted simulation studies to evaluate the performance of Generic ETUS in the presence of 30% malicious nodes and have compared it with ETUS routing protocols. The results show that Generic ETUS significantly improves the performance of ETUS in all metrics, packet delivery ratio and control overhead. The future research will focus on improving the generic ETUS performance by minimizing the innocent node booking.

REFERENCES

Bajaj, L., M. Takai, R. Ahuja, K. Tang, R. Bagrodia and M. Gerla, 1999. GloMoSim: A scalable network simulation environment. Technical Report 990027, University of California.

Georgiadis, L., M.J. Neely and L. Tassiulas, 2006. Resource allocation and cross-layer control in wireless networks. Found. Trends Networking, 1: 1-144.

IEEE, 1999. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE 802.11, August, 1999, Institute of Electrical and Electronics Engineers Inc., New York, USA.

Jayasingh, B.B. and B. Swathi, 2010. A novel metric for detection of Jellyfish reorder attack on ad hoc network. BVICAM's Int. J. Inform. Technol., 2: 15-20.

Jyoshna, G. and K.Y. Prasad, 2012. Removal of byzantine attacks in Ad hoc networks. Int. J. Adv. Res. Comput. Engin. Technol., 1: 272-276.

Kathirvel, A. and R. Srinivasan, 2011a. ETUS: Enhanced triple umpiring system for security and robustness of wireless mobile Ad hoc networks. Int. J. Commun. Networks Distrib. Syst., 7: 153-187.

Kathirvel, A. and R. Srinivasan, 2011b. ETUS: An enhanced triple umpiring system for security and performance improvement of mobile Ad hoc networks. Int. J. Network Manage., 21: 341-359.

Megha, A. and Y.K. Jain, 2011. Grayhole attack and prevention in mobile Ad hoc network. Int. J. Comput. Appl., 27: 21-26.

Rai, A.K. R.R. Tewari and S.K Upadhyay, 2010. Different types of attacks on integrated MANET-Internet communication. Int. J. Comput. Sci. Secur., 4: 265-274.

Raj, P.N. and P.B. Swadas, 2009. DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. Int. J. Comput. Sci., 2: 54-59.

Rani, L.S. and R.R. Sekhar, 2012. Detection and prevention of wormhole attack in stateless multicasting. In. J. Sci. Engin. Res., 3: 1-5.

Soldo, F., A. Le and A. Markopoulou, 2011. Blacklisting recommendation system: Using spatio-temporal patterns to predict future attacks. IEEE J. Sel. Areas Commun., 29: 1423-1437.

Tsou, P.C., J.M. Chang, Y.H. Lin, H.C. Chao and J.L. Chen, 2011. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. Proceedings of the 13th International Conference on Advanced Communication Technology, February 13-16, 2011, Seoul, Korea, pp: 755-760.

Yu, C.W., T.K. Wu, R.H. Cheng and S.C. Chang, 2007. A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. In: Emerging Technologies in Knowledge Discovery and Data Mining, Washio, T., Z.H. Zhou, J.Z. Huang, X.H. Hu and J.Y. Li *et al.* (Eds.). Springer, New York, USA., pp: 538-549.