International Journal of
Sensor Networks and Data Communications

Patil1 and Borade, Sensor Netw Data Commun 2014, 3:1
DOI: 10.4172/2090-4886.1000116

Review Article Open Access

Dynamic Cluster Based Intrusion Detection Architecture to Detect Routing Protocol Attacks in MANET

Sarika Patil[1] and Deepali Borade[2]*

[1]M.E (Computer Network), Computer Engineering Department, Flora Institute of Technology, Pune, Maharashtra, India
[2]Assistant Professor, Computer Engineering Department, Flora Institute of Technology, Pune, Maharashtra, India

Abstract

Mobile Ad-Hoc Networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station. MANET is more vulnerable to different types of attacks and security threats because of its characteristics of mobility and dynamic nature. Intrusion means any set of action that attempts to compromise the integrity, confidentiality, availability of resources. We are implementing EAACK secure acknowledge based IDS to remove the drawbacks of Watchdog. By using the schemes of EAACK we propose a cooperative, dynamic hierarchical intrusion detection architecture that addresses these challenges while finding specific and conventional attacks in MANET. The structural design is organized as a dynamic hierarchy in which data is acquired at the leaves and is incrementally aggregated, reduced, and analyzed as it flows upward toward the root. To maintain communications effectiveness, the hierarchy is automatically reconfigured as desired using clustering techniques in which cluster heads are selected based on topology and other criteria. The usefulness of the architecture is demonstrated via black hole attack scenarios in which attack is detected and removed. Reactive routing protocol is used as it provide better efficiency and hence to reduce the network overhead.

Keywords: Attacks; Dynamic Source Routing (DSR); Intrusion Detection System (IDS); Mobile Ad-hoc Network; Security

Introduction

A Mobile Ad-hoc Network (MANET) is a self- configuring and self-organizing network created without human intervention by a collection of mobile nodes. Each node is prepared with a wireless transmitter and receiver, allows communicating with other nodes in its same radio range. Each node must act as both a host and a router at the same time. The characteristics of MANETs are dynamic topology, mobility, security, power consumption, etc. Due to the mobility and dynamic nature of MANET, network is not protected. Intrusion Detection System (IDS) can be defined as the process of monitoring activities in system, which can be a computer or network system. In this, due to the restrictions of most MANET routing protocols, nodes in MANETs suppose that other nodes always assist with each other to transmit data. This supposition disappear the attackers with the opportunities to achieve major force on the network with just one or two compromised nodes. To tackle this problem, IDS should be added to develop the security level of MANETs. Intrusion detection can be used as a second wall of defense to defend the network from such problems. If the intrusion is found, a response can be started to avoid damage to the system. Due to dynamic nature of the MANETs, is vulnerable to different types of attacks and security threads. There are two techniques to secure MANET from different types of attacks. Prevention: mechanisms usually require encryption techniques to provide authentication, integrity, etc. Some proposals use symmetric algorithms, asymmetric algorithms, and one way hashing. Detection and Reaction: These are solutions that attempt to identify the malicious activities in the network and take actions against such nodes. e.g watchdog. In addition, IDS can also initiate a proper response to the malicious activity. Intrusion detection in MANETs is challenging task because of number of reasons. These networks change their topologies dynamically, lack attention points where traffic can be analyzed for intrusions; utilize self-configuring Multi party infrastructure protocols that are vulnerable to malicious attacks and rely on wireless communications channels that provide limited bandwidth and are subject to noise and discontinuous connectivity. To overcome these constraints, researchers have proposed a number of decentralized intrusion detection modified approaches specifically for MANETs. These approaches have focused on detecting malicious behavior with respect to MANET routing protocols and have provided little proof that they are applicable to a broader range threats, including attacks on conventional protocols, which also pose new problems in MANETs. This paper describes a dynamic hierarchical intrusion detection architecture proposed as the basis for all intrusion detection and sustaining activities in mobile ad hoc wireless networks. MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. The proposed solution is Dynamic Hierarchical Intrusion Detection Architecture to Detect Routing Protocol Attacks. Here we are going to study and analyze the well-known Black Hole attack.

The paper is organized as follows, section 4 describes literature survey and section 5 describes proposed system, section 6 describes conclusion of the paper.

Literature Review

Watchdog & Pathrater proposed by Marti et al. [1] which increases throughput of network in the presence of cooperated or malfunctioning nodes. Disadvantages are that it does not detect a misbehaving node in the presence of 1) ambiguous collisions,

***Corresponding author:** Deepali Borade, Assistant Professor, Computer Engineering Department, Flora Institute of Technology, Pune, Maharashtra, India, Tel. +09766347555; E-mail: deepali21@gmail.com

Received August 12, 2013; **Accepted** August 26, 2014; **Published** September 01, 2014

Citation: Patil S, Borade D (2014) Dynamic Cluster Based Intrusion Detection Architecture to Detect Routing Protocol Attacks in MANET. Sensor Netw Data Commun 3: 116. doi: 10.4172/2090-4886.1000116

2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping.

Huang and Lee [2] proposed a cluster based cooperative intrusion detection system which is capable of detection an intrusion and reveals the type of attack and attacker. Disadvantages are if the system does not implement clusters then the detection accuracy is worse. Need to prevent a compromised node be selected as cluster head. Not mentioned about false alarm rate.

Kejun liu et al. [3] proposed 2ACK scheme focuses the problem of detecting misbehaving links instead of misbehaving nodes. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. Disadvantage of 2ACK is higher routing overhead. This additional routing overhead is caused by the transmission of 2ACK packets.

TWOACK [4] detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. Disadvantages are the acknowledgment process required in every packet transmission process added unwanted network overhead.

AACK [5] is an end-to-end acknowledgment. Disadvantages are AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

EAACK [6] proposed by Elhadi et al., Malicious attackers can be detected by using Enhanced Adaptive Acknowledgement scheme. Compared to

RSA, DSA has more overhead. These techniques have drawbacks due to the collusions of packets and distribution of keys between nodes becomes overhead. The researchers have been studied on drawbacks of EAACK system such as key exchange problem and the hybrid cryptography problems. Our focus is study and removes the drawback of EAACK scheme such as partial dropping problem which does not completely removed by the EAACK system. Table 1 shows the comparative study of Various Misbehaving Techniques.

Umaparvathi et al. in [7] uses AODV to detect single node acting as a black hole. Group of nodes collectively &co- operatively detect black hole attack. Proposed system works on two-tier. Tier 1 detects single black hole node using verification message. Whereas tier 2 detect group of nodes creating black hole attack using number of Control messages and number of data packets.

Murugan et al. [8] has proposed cluster based technique to detect misbehavior nodes called black hole node, using cluster based technique and threshold cryptography. The proposed scheme has used Proactive Secret sharing technique to share secret key among nodes which is deployed along with threshold cryptography to provide more security.

In summary, the architecture proposed here is distinguished from prior research on intrusion detection for MANETs; the main focus of the architecture is to find the attacks on MANET using the hierarchical cluster based topology.

Proposed system

The proposed architecture is designed using EAACK- Enhanced Adaptive Acknowledge based secure intrusion detection system and by forming a clusters to mitigate routing protocol attack called black hole attack. Each cluster has cluster head to detect, observe and gives alert if an intrusion is detected. To implement the proposed architecture following are the modules.

1. Send packets from source to destination by encrypting the packet using RSA [9] and DSA [10] algorithm.
2. Design and develop schemes of EAACK [6] such as Acknowledgement, Secure-ACK and MRA (Misbehavior Report Authentication).
3. Apply this EAACK scheme on cluster based IDS to detect and remove the black hole routing protocol attack.

Module 1: Encryption technique by digital signature

In EAACK system all acknowledgment packets are authenticate, pure & verified. If the attackers made the forge acknowledgment packets then all the above three mode are weak. For this concern digital signature incorporated in proposed scheme. EAACK needs all acknowledgment packets are digitally signed before they are sends out and get verified till they are accepted.

The general steps of communication with the digital signature:

1) Applying hash function H on the message *msg* and compute the message digest *msg'*

$$H\ (msg)=d$$

2) The sender Bob needs to encrypt the message digest with his private key, the result is the digital signature.

$$Spr\text{-}Bob\ (d)=SigBob$$

3) This digital signature is append to the document and send it to Eve.

4) Eve computes the received message *msg'* with the help of hash function.

$$H\ (msg')=d'$$

5) Eve can verify the signature by applying Bob's public key. If Eve

Technique	Malicious Routing	Routing Overhead	False Misbehavior Detection	Packet Delivery Ratio	Detection & Prevention of Forged acknowledgement	Observation	Black Hole attack Detection & Removal
Watchdog	No	Low	No	Low	No	Self to Neighbors	No
Cooperative	Yes	Large	No	Medium	No	Neighbors to self	Yes
2ACK	Yes	Lesser than TWOACK	No	Large	No	Neighbors to self	Yes
TWOACK	Yes	Large	No	Medium	No	Neighbors to self	No
AACK	Yes	Lesser than above Technique	No	Large	No	Neighbors to self	No
EAACK	Yes	Same as AACK	Yes	Large	Yes	Neighbors to self	Yes

Table 1: Comparative study of Various Misbehaving Techniques.

check it out by comparing the d=d'. Then message is correct, it does not intercepted by intermediate nodes or attackers.

Module 2: Implementation of EAACK schemes

The approach of EAACK system was designed to deal with three of six weaknesses of watchdog scheme, particularly, false misbehavior, limited transmission power, and receiver collision.

The schemes of EEACK are Acknowledgement, Secure-ACK and MRA (Misbehavior Report Authentication) are described below.

ACK: ACK is an end-to-end acknowledgment EEACK scheme. The aim is to reduce the network overhead when no network misbehavior is detected. If source node send packet through intermediate nodes to destination, within predefined threshold source node has to get ACK from destination node. If source node does not receive ACK packet from destination node within defined threshold, source node switch to S-ACK mode and send out S-ACK data packet to detect misbehaving node in the route.

Figure 1 a) Shows flow of ACK scheme.

Secure Acknowledgment (S-ACK): In this scheme every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S- ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. If first node does not receive an acknowledgment packet with in a set of threshold time period, then next two consecutive nodes are reported as malicious, the misbehavior report is generated by first node & sent to the source node. Source node has to confirm misbehavior report S-ACK switch to MRA mode.

MRA: This scheme is designed to detect the misbehaving node with the presence of false misbehavior report. False misbehavior report can be generated by the attackers by reporting false to the innocent nodes as malicious as shown in Figure 2. The goal of MRA scheme is to authenticate whether the destination node has received the reported missing packet from a different route. In the MRA scheme source node searches for an alternate route to the destination node. When the destination node receives the MRA packet it searches and compares that the reported packet was received or not, if it is already received then it concludes that this is a false misbehavior report. Otherwise it will trust on report.

Module 3: Dynamic intrusion detection hierarchy

In cluster based IDS nodes are prearranged in a hierarchy with the top level nodes as Cluster Heads. The cluster heads have the tasks of (i) Data filtering and data fusion, (ii) Detection of intrusions and (iii) Security management. Being cluster based, improves the efficiency of IDS in terms of memory usage and network overhead.

Every node is responsible for using its own resident network and host based intrusion detection mechanisms to protect itself. Moreover, nodes are assigned intrusion detection responsibilities to help protect other nodes in the network. These responsibilities include monitoring, logging, analyzing, and reporting data at various protocol layers.

General Steps:

1. All nodes in the network have a capability to detect local intrusion.

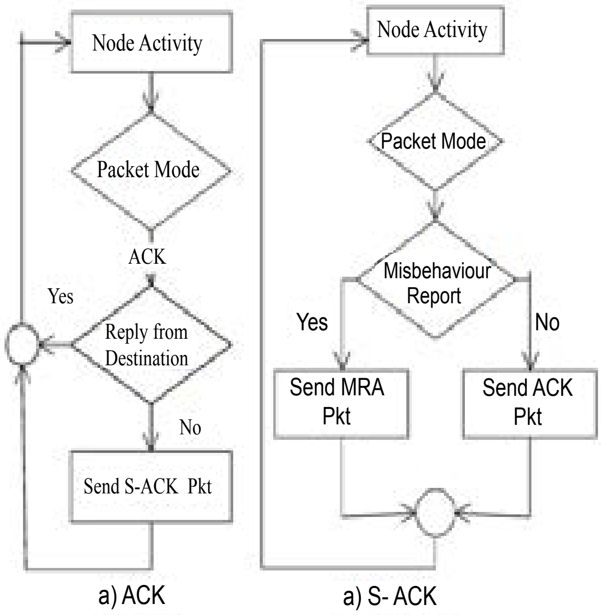

Figure 1: Flowchart of EAACK Schemes a) ACK b) S-ACK.

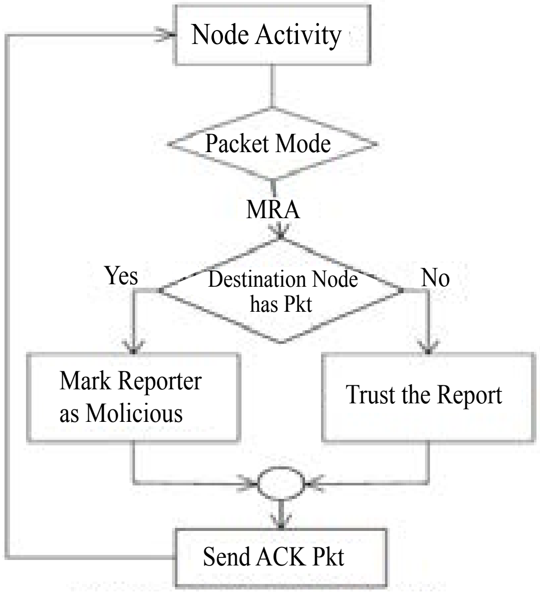

Figure 2: Flowchart of EAACK Schemes-MRA.

2. Observations of each node to detect misbehavior from all of its intermediate nodes.
3. Successfully aggregate this misbehavior by forwarding it to cluster head.
4. Analyze the aggregated observations to detect routing protocol attack such as black hole.
5. If intrusion is detected generates an alert forward it to all the nodes in the clusters.

Implementation and demonstration

As module 3 describes how the exact the system works for finding the routing protocol attacks in MANET. The key progress of a hierarchy is scalability to huge networks. Since it can provide fast efficient detection for local cooperative attack, and also allows for data sharing. An example of this structure is shown in Figure 3. Nodes denoted with a "1" are the representatives of first level clusters. Arrows pointing to these nodes begin from the other (leaf) nodes in their cluster that report to them. Similarly, arrows from first level representatives to their second level representative (annotated with a "2"), show the composition of one of the second level clusters. The arrow from the '2' level representative to the '3' level representative shows that the former is a member of a third level cluster; other members of that cluster are outside the scope of the Figure 1.

If there is single point of failure, one or more members of the highest level cluster are designated as backup representatives. This infrastructure allows intrusion detection observations to be gathered efficiently from the entire network.

Mitigation of black hole attack

There are two types of attacks in MANETs such as passive and active attacks. In passive attacks, packets including secret information might be overheard something, and it violates confidentiality. In active attacks, containing introducing packets to unacceptable destinations into the network, removing packets, changing contents of packets, and masquerading as other nodes violate security criteria. Classification of misbehavior attack is as shown in Figure 4. The proposed architecture identifies routing misbehavior called as black hole attack. There are two types of routing protocols are used in MANET proactive and reactive. Proactive routing protocols maintain routing table and static in nature [11].

Reactive routing protocols are on-demand routing [11] and dynamic in nature e.g. AODV [12] & DSR [13]. Figure 5 explain the example of black hole attack using AODV routing protocol. Source node 1 broadcasts an RREQ (Route Request) message to discover a route for sending packets to destination node 5. An RREQ broadcast from node 1 is received by neighboring nodes 2, 3 and 4. However, malicious node 4 sends an RREP (Route Reply) message immediately without even having a route to destination node 5.

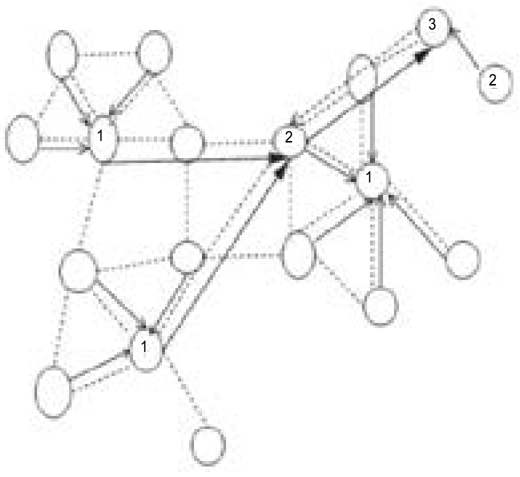

Figure 3: Dynamic Intrusion Detection Hierarchy.

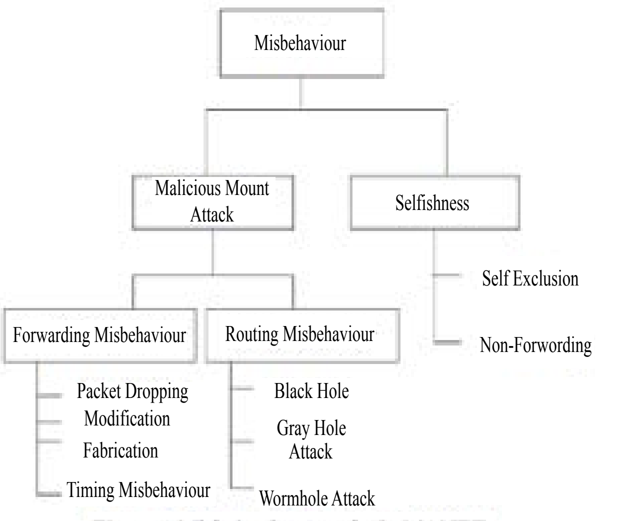

Figure 4: Misbehaviour Attacks in MANET.

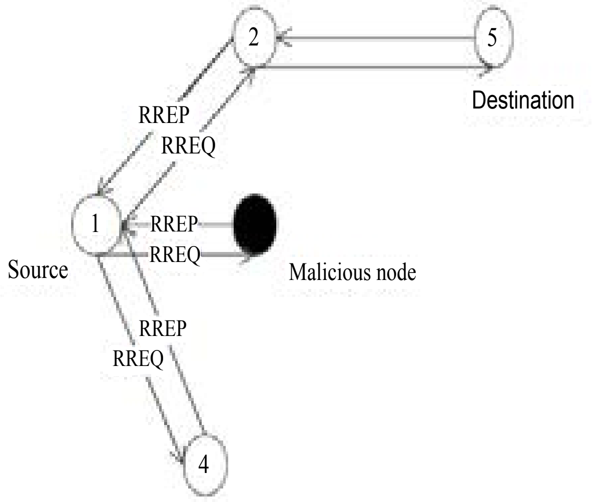

Figure 5: Black Hole Attack.

An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on. Proposed architecture works on Hierarchal based IDS in which nodes are divided in clusters. Node with maximum 1 hop count is chosen as Cluster Head (CH). AODV routing protocol has modified using cluster based technique to detect hijacked node causing black hole attack inside network.

Let us suppose N1 be the source node, N10 is the destination node as shown in Figure 6 which can be either in same cluster or different cluster. IMn be the intermediate nodes where n= 2, 3, 4… During route discovery phase source node N1 request cluster head (CH1) to

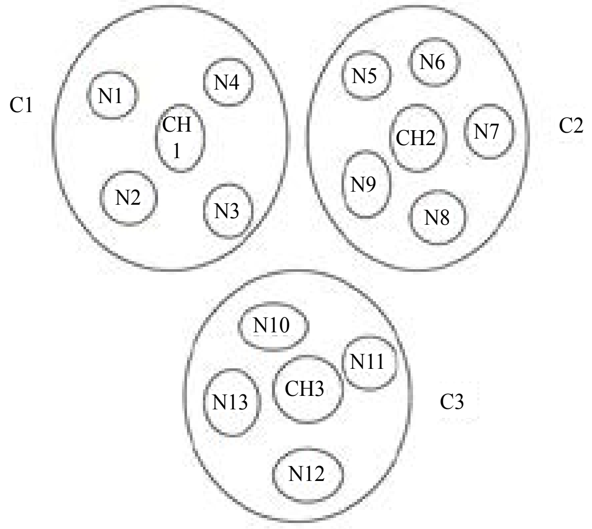

Figure 6: Cluster of Nodes.

issue certificate. CH issues certificate to source node, after checking its trust value. Source node broadcast RREQ (route request) to all its neighbors. RREQ would be of following format: RREQ< IPs, IPd, IDb, Seqs, Seqd, Cert, Hop_count >

Here IPs, IPd, is the IP address of source and destination respectively. IDb denotes the broadcast Id, Cert represents Certificate issued by Cluster Head. Hop_count depicts number of nodes message have passed.

In proposed method all the nodes receiving data packet send acknowledgement to the node from which it received. If source node receives acknowledgement from destination within threshold time, path is found to be secure against black hole node and originator takes no action. Otherwise source starts verifying nodes.

Suppose in the Figure 6. N5 is the source node and N9 be the destination node and N6,N7,N8 are the intermediate nodes whose addresses has been stored by N5.N5 node unicast the verification message to N6,N7,N8 and N9 upon receiving this each intermediate node send TRUE or FALSE, to the source node. Suppose N6 replies TRUE, N7 and N9 replies FALSE

& N8 does not reply in that case N8 is act as malicious (black hole node) and it does not forward the packets. Alarm has been raised by source node N5, and N8 node excluded or removed from network.

Proposed work algorithm

Description: The algorithm mentioned below implements cluster based technique to detect malicious node i.e. node causing black hole attack in network. The AODV routing node protocol used to test the functionality and to evaluate the performance.

The algorithm is implemented in two phase; route discovery phase of AODV and data packet sending phase.

Input = {Source_ip, Destination_ip, Data_packet} Output = {Attacker_node}

A. Route discovery phase

```
Begin
1. Get certificate CERT from the cluster head
2. Broadcast RREQ packets to all neighbors i.e., intermediate nodes IMn
3. if (IMn no route to destination)
then
Rebroadcast RREQ to all neighbors. Append self IP address
Reverse_Path_Pointer = (received
RREQ source || source node)
hop_count++
end if
else go to step 4
4. if(IMn.isDestination())
then
unicast – RREP to next hop towards destination
end if
else go to step 5
5. if(IMn : route to destination exists)
then
send RREQ packet towards destination
update the routing table
end if
End
```

After the RREP packet is reached the source, it chooses IMn with higher sequence number and then extracts the path details from the packet and stores in the repository tagging with respect to destination.

B. Data packet sending phase

```
Begin
1. packetPath[] = route path from repository for destination
2. send DATA_PACKET to packetPath[0]
3. RREPThreshold = T
4. if (RREP received within RREPThreshold)
  then
  path doesn't contain malicious end if
node
else go to step 5
5. Activate node verification service.
```

for each node : storedNodes[] unicast verification message collect verification message result

```
if (!verification_message)
node.nextNode    =    malicious (black hole)
6. Alarm has been raised by source node
7. Broadcast node elimination message to
all stored Nodes[]
End
```

C. Mathematical model

1. Problem statement: Implement cluster based technique to detect and eliminate malicious node from the network.

2. Mathematical module:

1) C is set of all clusters in the network

C = {c1, c2, c3, …}

2) CH is set of all cluster heads in clusters

CH = {ch1, ch2, ch3, …}

3) CN is the set of all nodes which are not cluster heads

CN = {cn1, cn2, cn3, …}

4) RN is the set of all nodes within the route from a source to destination

PN = {pn1, pn2, pn3, …}

5) P is the set of process constituting the execution of technique proposed

P = {P1, P2, P3} Where,

a. P1 = {s1,s2,s3} Where,

s1 = {i|i is to get route from repository for particular destination}

s2 = {j|j is to create a data packet}

s3 = {k|k is to send packet to destination along the route}

b. P2 = {s1,s2} Where,

s1 = {i|i is process in waiting state till the threshold time is reached}

s2 = {j|j is collect acknowledgements from intermediate nodes along route}

c. P3 = {s1,s2} Where,

s1 = {i|i is process to activate node verification service}

s2 = {j|j is collect verification unicast messages}

s3 = {k|k is to analyze the received verification results}

s4 = {l|l is to broadcast drop node message to all verified nodes}

3. NP hard or NP complete: The results are comes into the NP complete because in particular time it will give the result. For the decision problem, so that it will give the solution for the problem within polynomial time. The set of all decision problems whose solution can be provided into polynomial time by using the given algorithm

4. Functional assumptions: Malicious node always tries to hide itself and preserve its identity. Hence, it doesn't reply properly for the unicast verification messages send to all nodes during the node verification service.

Input: {Nodes within the route, source-destination tuple}

Output: {Black hole causing node free network}

Success: {Black hole causing node detected accurately and eliminated from the network}

Failure: {Black hole attack persists}

Conclusion

In this paper, we have designed and developed the cluster based EAACK architecture to detect and remove black hole attack in MANET. Clusters are formed in the network and cluster heads (CH) are selected manually for experimental result. The digital signature has incorporated into the data packet as well as the acknowledgement packet by using RSA and DSA algorithm. The AODV routing protocol used to test the functionality and to evaluate the performance. Routing Overhead can be increased in some cases but it improves the packet delivery ratio.

Future Work

In the future we will extend this research by comparing the experimental results with existing Intrusion Detection Systems as well as with different types of network attacks. As this is acknowledgement based system which generates more networks overhead, that can be improved with other technique.

References

1. Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,.Proceedings of the 6th Annual International Conference.
2. Huang Y, Lee W (2003) A cooperative intrusion detection system for ad hoc networks. Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03) pp.135-147.
3. Bansal, Baker, Kejun Liu, Jing Deng, Pramod K, et al. (2007) An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs. IEEE transactions on Mobile Computing, 6:448-502.
4. Balakrishnan K, Jing Deng, Varshney VK (2005) TWOACK: preventing selfishness in mobile ad hoc networks. Proceedings of Wireless Communications and Networking Conference IEEE, 4:2137-2142.
5. Sheltami T, Roubaiey AL, Shakshuki E, Mahmoud A (2009) Video transmission enhancement in presence of misbehaving nodes in MANETs. Int J Multimedia Syst 15:273–282.
6. Elhadi M, Shakshuki, Nan Kang, Tarek R, Sheltami EAACK—A Secure Intrusion-Detection System for MANETs (2013) IEEE Trans Industr Inform 60:1089-1098.
7. Umaparvathi M, Dharmishtan K, Varughese (2012) Two Tier Secure AODV against Black Hole Attack in MANETs. Eur J Scientific Research 72:369-382.
8. Murugan R, Shanmugam A (2012) Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks. Int Comp Sci Secur 6: 188.
9. Rivest R, Shamir A, Adleman L (1983) A method for obtaining digital signatures and public-key cryptosystems. Commun, ACM, 21: 120–126.
10. Gaithersburg MD (2009) Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-3, National Institute of Standards and Technology, USA.
11. Abolhasan M, Wysocki T, Dutkiewicz E (2004) A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2: 1–22.
12. Perkins C, Royer E (1999) Ad-hoc on-demand distance vector routing, in Mobile Computing Systems and Applications, Proceedings.WMCSA'99, Second IEEE Workshop on IEEE: 90–100.
13. Johnson D, Maltz D (1996) Dynamic Source Routing in ad hoc wireless networks, in Mobile Computing. Norwell, MA: Kluwer. 5: 153–181.