International Journal of Research in Engineering & Technology (IJRET)
Vol. 1, Issue 1, June 2013, 35-44
© Impact Journals

INTELLIGENT INTRUSION HANDLING FOR MITIGATING MANET ROUTING ATTACKS

A. PRIYADHARSHINI

Research Scholar, Department of CSE, Shreenivasa Engineering College, Dharmapuri, Tamil Nadu, India

ABSTRACT

Mobile Adhoc Networks are autonomous and decentralized wireless systems. Security in MANET is one of the most important concern for basic functionality of the network. MANETs often suffer from security attacks because of its characteristics like lack of fixed infrastructure, dynamism of topology, resource constraints, open medium and no clear defense mechanism. Routing in such a network becomes more complex because of its dynamic topology. So routing attacks have become a challenging task in MANET. In this paper, I propose a intelligent intrusion handling mechanism with an adaptive isolation method to resolve routing attacks in MANET. The intrusion handling mechanism make use of Extended Dempster Shafer theory that treat attacks according to their importance. The mechanism make use of Optimized Link State Routing protocol that reduces the possible overhead in the network protocol by using Multipoint Relays.

KEYWORDS: Routing Attacks, Extended Dempster Shafer Theory, OLSR

INTRODUCTION

In recent years the widespread availability of wireless communication and handheld devices has simulated research on self-organizing networks that do not require a preestablished infrastructure. Adhoc networks can be subdivided into two classes, one is static and another one is dynamic. In static adhoc networks once the position of the nodes are fixed it can't be changed. But in Mobile Adhoc networks the position of the nodes can change frequently.

MANET is a self-configuring infrastructureless network of mobile nodes without any wired link. Each node(device)in the MANET move independently in any direction and can join or leave the network at any time. These nodes act as end systems as well as routers. Mobile Adhoc Networks are utilized to setup wireless communication in environments without a predefined or centralized administration. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. As each node plays a router role while transmitting data in MANET, routing attacks have become more common in MANET. So routing has become a more challenging task. In this paper, I use OLSR(Optimized Link State Routing)protocol which is proactive in nature to overcome routing issues in MANET.

There are many challenges in MANET. They are

- **Secrecy:** Secrecy is to keep information out of unauthorized users.
- **Authorization:** Authorization is finding out if the person, once identified, is permitted to have the resource.
- **Authentication:** Authentication is any process by which verification is done for an entity is one that it claims to be.
- **Non-Repudiation:** Provides protection against denial by one of the entities involved in a communication.
- **Integrity Control:** This is to ensure that the messages that are received were the ones which are really sent and not something that is modified in transit.

- **Privacy:** Keep systems from finding out about users.
- **Confidentiality:** The principle of confidentiality specifies that only the sender and the intended receipient should be able to access the contents of a message.
- **Access Control:** The principle of access control determines who should be able to access what.
- **Availability:** The principle of availability states that resources should be available to authorized parties at all times.

To address these issues I propose an intrusion handling mechanism with adaptive isolation method that use Extended Dempster Shafer theory.

CLASSIFICATION OF ATTACKS ON MANET

Attack is an intelligent act that deliberate attempt to evade security services and violate the security policy of a system. There are two types of attack.1. Passive attack: Attempts to learn or make use of information from the system but does not alter system resources.2.Active attack: Attempts to alter system resources or affect their operation. Further attacks are classified into Insider attack: Is an attack initiated by an entity inside an organization and Outsider attack: Is an attack initiated by an entity outside an organization ie by an unauthorized person. Among these attacks routing attacks could cause significant damage to MANET.

Routing Attacks

The attacker node floods the network with bogus route creation packets to fake(non existing)nodes or simply sends excessive route advertisements to the network. As the topology of MANET is dynamic, routing in such a network is more challenging. So attacker can easily launch an attack.

Attacks during Route Discovery

Routing attacks that target the route discovery phase such as routing message flooding attacks, routing table overflow, routing cache poisoning, routing loop etc.

Attacks during Route Maintenance

Routing attacks that target the route maintenance phase by broadcasting false control messages such as link-broken error messages which cause the invocation of the costly route maintenance or repairing operation. Attackers could take advantage of the mechanism to launch attacks by sending false route error messages.

Attacks during Data Forwarding Phase

In this scenario the malicious nodes participate in routing protocol route discovery and maintenance phase, but in the data forwarding phase they do not forward data packets according to the routing table. Malicious nodes simply drop data packets, modify data content, replay or flood data packets.

Attacks on Routing Protocols

These attacks target particular routing protocols. For example in AODV(Adhoc On-Demand Distance Vector)the attacker may advertise a route with smaller distance than the actual distance .In DSR(Dynamic Source Routing) the attacker may modify RREQ(route request) or RREP(route reply) packets.

Wormhole Attack

It involves the cooperation between two attacking nodes. One attacker captures routing traffic at one point of the network and tunnels it to another point in the network that shares a private high speed communication link between the attackers and selectively injects tunnel traffic back into the network. This tunnel between two colliding attackers is referred as a wormhole.

Blackhole Attack

The attacker node injects false route replies to the route requests claiming to have the shortest path to the destination node whose packets it wants to intercept. The attacker node is then in a position to misuse or discard any or all of the network traffic being routed through it.

Byzantine Attack

A compromised node or set of compromised nodes carry out attacks such as routing loops, selectively drop packets or forward packets through non-optimal paths.

Node Repudiation

Where the communicating entities denies the sending or receiving of the message.

Rushing Attack

If a fast transmission path exists between two ends of a wormhole the tunneled packets can propagate faster than those through a normal multihop route. This is known as rushing attack. The attacker node initiates a route discovery for the target node. If the ROUTE REQUEST by the attacker is the first to reach each neighbor of the target, then the route discovered will include a hop through the attacker.

Resource Consumption Attack (Sleep Depravation)

The attacker node continually requests for either existing or non-existing destinations forcing the neighboring nodes to forward these request packets.

Location Disclosure Attack

With simple monitoring approaches an attacker is able to discover the location of a node and the structure of the network.

Flooding Attack (Routing Table Overflow)

The attacker node floods the network with bogus route creation packets to non-existing nodes or simply sends excessive route advertisements to the network.

Impersonation Attack

The attacker node impersonates a legitimate node and sends false routing information masked as trusted node.

Node Isolation Attack

The attacker prevent link information of a specific node(isolate)and other nodes will not able to send data to these nodes.

Routing Table Poisoning Attack

It results in selection of non-optimal routes,creation of routing loops and even partitioning the network by injecting a RREQ packet with a high sequence number.

Blackmail

Nodes usually keep information of perceived malicious nodes in a blacklist.An attacker may fabricate such reporting message and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

Snare Attack

Attacker physically compromise a node and the compromised node could be used to lure a Very Important Node(VIN).

The Invisible Node Attack

Any node that effectively participates in that protocol without revealing its identity is an invisible node and the action and protocol impact is termed as INA.

ADHOC ROUTING PROTOCOLS

The routing protocols for adhoc wireless network should be capable to handle a very large number of hosts with limited resources such as bandwidth and energy. The main challenge of routing protocols is that they must also deal with host mobility(the hosts can appear and disappear in various locations).All hosts of the adhoc network act as routers and participate in the route discovery. The routing protocol needs to have following qualities in order to be effective.

- Distributed operation

  A host can enter network whenever it wants.

- Loop-freedom

  To prevent the host sending information uselessly.

- Demand-based operation

  Decrease traffic.

- Proactive operation

  Used when there is enough resources and bandwidth.

- Security

  Taken in consideration as mobile devices are vulnerable to snooping because of the broadcasting.

- Sleep period operation

  To reduce the energy used by hosts.

- Unidirectional link support

  In mobile network, links are unidirectional and hence ULS is essential.

  Routing protocols are divided into three categories.

- Proactive routing protocols

  The primary characteristic of proactive approaches is that each node in the network maintains a route to every node in the network at all times.

- Reactive routing protocols

  In which the routes are created and maintained only when they are needed.

- Hybrid routing protocols

  It combines the uses of both proactive and reactive routing protocols.

Optimized Link State Routing Protocol

OLSR is a proactive routing protocol, so that the routes are immediately available when needed. To reduce the possible overhead in the network it uses Multipoint Relays(MPR).The message is broadcasted only to MPR nodes. Control messages exchanged between nodes are:

- Hello messages-only to MPRs.
- Topology Control (TC)-to all hosts.

Neighbour Sensing: Hello messages are used for neighbor sensing. Each node periodically transmits a Hello message that contains a list of all neighbors. Associated with each neighbor is an attribute indicating the directionality of the link to that neighbor. The node is labeled symmetric if the link to the neighbor is bidirectional or asymmetric if a Hello has been received from that node but the link has not been confirmed as bidirectional.

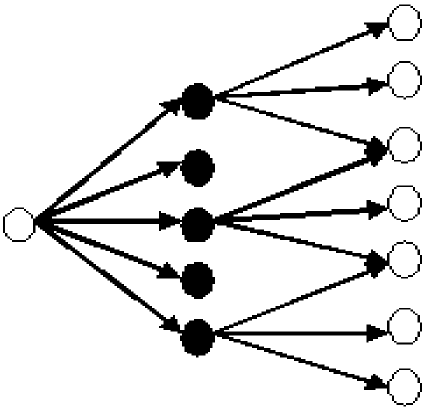

Figure 1: MPR Flooding

When a node receives this Hello message from each of its neighbors, it obtains knowledge of its two-hop neighbor set at that point in time. Further, if its own address is listed in the Hello message, it knows the link with that neighbor is bidirectional. The MPR must be symmetric neighbors. It can then update the status of that neighbor to be symmetric. In order to exchange the topological information the host that are selected as MPR need to sent the Topology Control(TC) message. Figure 1 shows MPR flooding.

The host maintains the routing table, the table entries have the following information: destination address, next hop(next address), number of hops to the destination and local interface address.

Advantages

- It does not need central administrative system to handle its routing process.The flooding is minimized by the MPRs,which are only allowed to forward the topological messages.
- The messages are sent periodically and the delivery does not have to be sequential.

- It is easy to integrate the routing protocol in existing OS.
- It has advantage in networks with high density and dynamic traffic where reactive protocols performs well only in static traffic.

EXTENDED DEMPSTER SHAFER THEORY

Dempster Shafer Theory

It enables us to present subjective knowledge(retrieved from previous experience) and objective evidence(obtained from observation) with probable reasoning, where previous approaches such as Fuzzly MLS have considered only subjective knowledge and objective evidence into account.

The probability that “the detected attack is X” is indicated by a “confidence interval”,

$[\mathrm{Belief}_i(X),\mathrm{Plausibility}_i(X)]$ (1)

The lower bound of the confidence interval is the belief confidence, which accounts for all evidence E_k that supports the given proposition “attack X”.

$\mathrm{Belief}_i(X)=\sum m_i(E_k)$ (2)

$E_k \subseteq X$

The upper bound of the confidence interval is the plausibility confidence,which accounts for all the observations that do not rule out the given propagation.

$\mathrm{Plausibility}_i(X) = 1-\sum m_i(E_k)$ (3)

$E_k \cap X=\varphi$

Disadvantages

- **Associative:** The order of the received information does not impact the result.
- **Nonweighted:** All evidences are trusted equally.

Weighted Dempster-Shafer Evidence Combination Rule

In Dempster-shafer(D-S) theory “equal trusting” is followed but it is useful for situation when both observations have the same accuracy estimates. Incase of unequal confidence, weighted Dempster Shafer theory is used.

The basic idea is: The theory uses historically estimated correctness rate as the reference to decide how much to trust current estimation from its current observation.

So, the equation becomes

$\mathrm{Belief}_i(X)=\sum w_i\, m_i(E_k)$ (4)

$E_k \subseteq X$

and

$\mathrm{Plausibility}_i(X) = 1-\sum w_i\, m_i(E_k)$ (5)

$E_k \cap X = \varphi$

Where w_i denotes the corresponding weight or importance factor.

Importance factor: IF is a positive real number associated with each evidence that denotes how much the attack is important.

INTRUSION HANDLING

When an intrusion occurs, the intrusion handling restores the system to comply with the site security policy(defines what is correct) and taking actions against the attacker. In this approach the attacks are treated according to their importance using Extended Dempster Rule of Combination by various steps. The process is illustrated in figure 2.

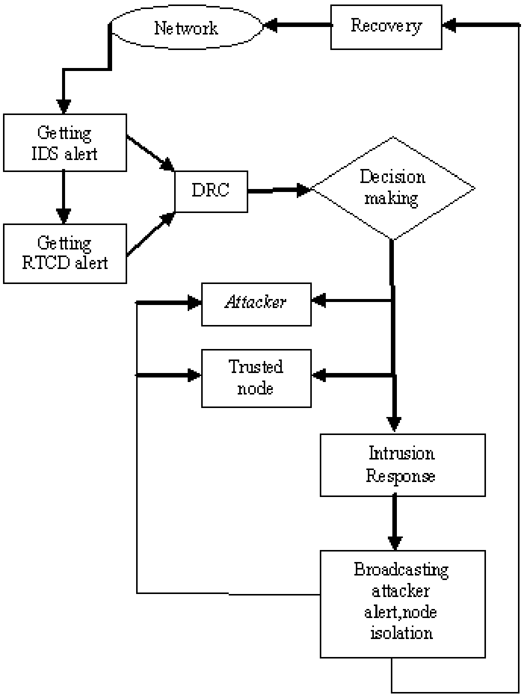

Figure 2: Intrusion Handling Steps

The steps are follows

Preparation for an Attack

This step occurs before any attack is detected. It establishes procedures and mechanisms for detecting and responding to attacks.

Identification of an Attack

This triggers the remaining phases. Evidence for an attack is collected from Intrusion Detection System and Routing Table Change Detector. A wireless IDS monitors and analyses wireless network traffic looking for potential problems with wireless protocols.

In addition to traditional IDS, the wireless IDS can also detect the following:

- Unauthorized WLANs.
- Poorly secured WLAN devices.
- Unusual usage patterns.

- The use of wireless network scanners.
- Denial of Service(DOS) and node repudiation attack.
- Impersonation and man-in-the-middle attack.

As some IDS produce false alarm (an event triggers an alarm when no attack is in progress),the wireless IDS provides evidence(alert) with a confidence value which is also known as importance factor.

These information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory.

Confinement of the Attack

This step limits the damage as much as possible. A flexible decision making is done during this phase which takes risk estimation and risk tolerance into account. The attacks are identified and attacker nodes are separated from trusted node.

Eradication of the Attack

This step stops the attack and block further similar attacks. Intrusion response is carried out during this phase which includes node isolation and broadcasting attacker alert.

During node isolation the neighbors of attacker node bands the service neither sending packets to it nor accepting any packets from it. It can be done temporarily or permanently. In temporary isolation once the node is isolated it can join the network later time but in permanent isolation the node is isolated permanently.

During broadcast an alert about the attacker node is given to the trusted nodes.

Recovery from the Attack

The system restores the system to a secure state and possible recovery actions are taken like routing table recovery .

During routing table recovery the table entries are corrected. It can be done both locally and globally. In local routing table recovery victim nodes detect the attack and automatically recover its own routing table. Whereas in global routing table recovery victim nodes update their routing table based on corrected routing information by other nodes in the network.

Follow-up to the Attack

This step involves taking action against the attacker, identifying problems in handling of the attack and recording lessons learned.

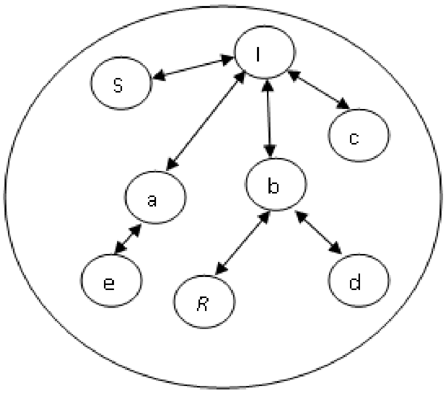

Figure 3: An Attack Scenario in MPR Nodes

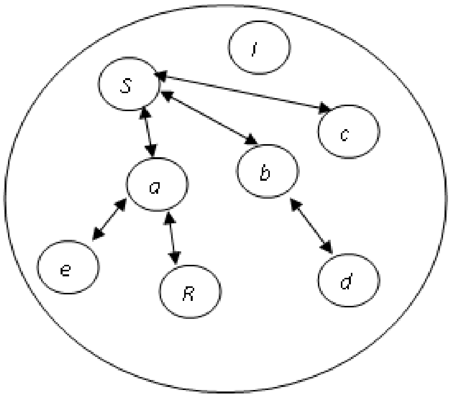

Figure 4: After Node Isolation

An attack scenario in MPR nodes is illustrated in Figure 3.And the attacker node is isolatated in Figure 4.The Intruder(I) node gains all routing information from the Sender(S) node and on behalf of the sender node it sends data packets or any request packets towards the R(receiver) node. After identification of an attack the intruder node is isolated from the network. No data packet is forwarded or received from the intruder node.

CONCLUSIONS

A new intrusion handling approach is proposed that resolve MANET routing attacks efficiently. Additionaly the proposed approach resolves node repudiation and DOS attack by using wireless Intrusion Detection System which is a drawback of other IDS. The response mechanism is adaptive in nature and handle attacks according to their importance. As OLSR protocol is proactive in nature there is no overhead of route creation and route maintainance. And in OLSR all the packets are forwarded only to MPR nodes hence reduce traffic overhead with limited resource constraints such as limited power capacity, memory, bandwidth, computational capacity etc.

REFERENCES

1. P. Cheng, P. Rohatgi, C. Karger, G. Wagner, and A. Reninger, “Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control,” Proc.28th IEEE Symp. Security and Privacy, 2007.

2. T. Clausen and P. Jacquet “Optimized Link State Routing Protocol (OLSR),” RFC 3626, IETF Network Group,October 2003.

3. P . Jacquet, A. Laouiti,P. Minet and L. Viennot “Performance of multipoint relaying in ad hoc mobile routing protocols,” Networking 2002.Pise(Italy)2002.

4. Y. Zhang and W. Lee,“Intrusion detection in wireless ad-hoc networks,” in Proceedings of Mobicom 2000,pp.275-283, Aug 2000.

5. H. Deng, W. Li, and D.P. Agrawal, “Routing security in ad hoc networks,” IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

6. C. Tseng, T. Song, P. Balaaubramanyam, C.Ko, and K. Levitt, “A Specification-Based Intrusion Detection Model for OLSR,” Proc. Ninth Int’l Symp. Recent Advances in Intrusion Detection (RAID ’06), pp.249-271, 2006.

7. G. Shafer, A Mathematical Theory of Evidence, Princeton Univ., 1976.

8. Y. Sun, W. Yu, Z. Han, and K. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad

Hoc Networks," IEEE J. selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.

9. L. Sun, R. Srivastava, and T. Mock, "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," J. Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006.

10. C. Mu, X. Li, H. Huang, and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08),pp. 35-48, 2008.

11. K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.[9] L. Zadeh, "Review of a Mathematical Theory of Evidence," AIMagazine, vol. 5, no. 3, p. 81, 1984.

12. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719, May 2010.

13. S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection (RAID '07), pp. 127-145, 2007.

14. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.

15. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor Fusion Using Dempster-Shafer Theory," Proc.IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.