ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Authorization Enforcement Facility in MANETs by Combining Static and Dynamic Condition

Gowthami[1] A, Persi Pamela I[2]

Assistant Professor, Department of Information Technology, Kingston Engineering College, Vellore, India[1,2]

Abstract: As MANETs are highly vulnerable to attacks due to its dynamic infrastructure, there may occur several attacks. Among those attacks routing attack is the most severe one. To systematically cope up with this routing attack, Risk Aware Response Mechanism is used .In these mechanism IDS is used which detects malicious activities caused by malicious nodes, Based on the risk of attack ,temporary decision is made whether isolation is needed or not .IDS used in risk aware response mechanism is static based approach .Hence rule set in IDS has to be updated often by the network administrator if there are any new emerging attacks. In this paper ,we propose a Authorization Enforcement Facility which uses risk as an input to determine how much a source node can be trusted. AEF considers both static approach as well as dynamic conditions in order to achieve better security and allow only secure communication to takes place between source and destination.

Keywords: Mobile Adhoc Networks, Risk Aware, Intrusion Detection System, security, Authorization Enforcement Facility

I. INTRODUCTION

Mobile Adhoc Networks (MANET) is a collection of mobile nodes and all those mobile nodes communicate with each other via wireless links either directly or relay on other nodes as routers. It does not need any predefined infrastructure and each and every node in the MANET environment are distributed and they does not have any centralized control. A mobile node dynamically keeps on changing due to mobility of nodes. MANET contains more number of mobile nodes within the network and they do not have any access point. The main goal of mobile adhoc networking is to extend mobility in to the realm of autonomous mobile, wireless domains. Each mobile node relies on each other for establishing communication within the network, and hence each mobile node plays a router role. Main advantages of MANETs are, the network can be set without any pre-existing infrastructure and can be set up at any place and any time. They provide access to information and services regardless of geographic position.

Routing is the act of moving data from source to destination in an internetwork. One of the important factors to be considered is, in between source and destination there must be at least one intermediate node for routing the data packet or information. Routing is mainly classified in to two types ,they are Static Routing and Dynamic Routing. Static Routing refers to the strategy for routing that are being stated manually in the router. It maintains a routing table usually written by a network administrator. This routing table doesn’t depend on the state of the network status, i.e it does not depend on whether the destination is active or not. Dynamic routing refers to the strategy that is being learnt by the exterior or interior routing protocol. The routing mainly depends on the network state i.e. based on the activeness of destination, the routing table gets affected.

Routing protocols for MANETs can be classified as Proactive or Table-Driven routing protocol, Reactive or On-Demand routing protocol and Hybrid routing protocol.

A. *Proactive Routing Protocol*

In proactive Routing Protocol, each node maintains routing information to every other node in the network. All the routing information are usually kept in a number of different tables. These routing tables are periodically updated, when ever topological changes occur in the network. This type of routing protocols may waste bandwidth since control messages are sent out unnecessarily when there is no traffic. The main advantage of using this type of routing protocol s is that host can quickly obtain route information and they quickly establish a session. Some of the examples of proactive routing protocols are OLSR, DSDV, FSR, and WRP.

B. *Reactive Routing Protocol*

Reactive routing protocol or On-Demand Routing Protocols execute the path finding process and routing information would be exchanged only when a node wants to communicate with a destination. Some of the on-demand routing protocols are DSR, AODV, TORA, LAR, ABR. The main disadvantage of using this type of protocols is, it finds a route on demand by flooding the network with Route Request packets and it takes high latency time in route finding, network clogging may occur due to excessive flooding.

Mobile Adhoc Networks are highly vulnerable to attacks due to dynamic infrastructure .Their topology keeps on changing due to the mobility of nodes .Due to changes in the topology, they may lead to changes in wireless link connections. Several attacks would occur within the Mobile Adhoc networks. Some of the attacks are limited transmission range, control overhead, routing attacks, bandwidth wastage, time varying wireless link characteristics, broadcast nature of wireless medium, hidden terminal problem, packet losses due to transmission errors, mobility induced route changes, frequent network partitions. Among them, routing Attacks is one of the critical one. To reduce this routing attacks, several intrusion response techniques [8],[11] were used. Intrusion Response technique may result in some binary or naive response decisions. Naive responses would cause unexpected network partitioning causing damage to the network infrastructure.

The rest of the document is organized as follows: In Section II, related works are reviewed. Section III which describes about existing risk aware response mechanism and decides whether isolation is needed or not in the presence of malicious node. Section IV describes about the problem that are occurring in current mechanism. Section V describes the proposed Authorization Enforcement Facility for achieving better security in the presence of malicious node and enhancing the existing risk aware approach. Finally in Section VII conclusion and future work are discussed.

II. RELATED WORK

Mobile Adhoc Networks contains more number of mobile nodes, among those nodes some times there may be presence of malicious nodes or attackers so, automatically throughput gets affected .To improve throughput , two techniques were used based on dynamic conditions[1] and they are Watchdog and PathRater. Watchdog detects the presence of malicious node and PathRater would avoid sending data packets through those nodes. Authenticated Routing for Adhoc Networks (ARAN)[2], which detects and protects against malicious actions caused by third parties and peers in one particular ad hoc environment. ARAN introduces message integrity, authentication, and non-repudiation to an ad hoc environment as a part of a minimal security policy. Secure Efficient Adhoc Distance vector routing protocol (SEAD) [3],is based on the design of the Destination Sequenced Distance Vector routing protocol. This protocol makes use of one-way hash functions and they helps in reducing the CPU processing capability and guarding the network against Denial-of-Service attacks in which an attacker tries to cause other nodes to consume excess bandwidth. SEAD protocol is robust against multiple uncoordinated attackers who are creating incorrect routing state in other nodes. Intrusion detection system[4], which monitors all misbehaving nodes within the network. Intrusion Detection System is defined as the automated detection and it generates an alarm to alert the security at a location, if there is chances of occurring any suspicious activities.IDS is a defence system that detects all hostile activities in the network and it tries to prevent such activities which may be compromising system security. Ariadne protocol [5], which provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptographic operations. Ariadne operates on demand, dynamically discovering routes between nodes only as needed ; the design is based on the basic operation of the DSR protocol. The security mechanisms which designed are highly efficient and general, so that they should be applicable for securing a wide variety of routing protocols. Distributed Evidence-driven Message Exchanging intrusion detection Model (DEMEM) [6], allows the distributed detector to cooperatively detect routing attacks with minimal communication overhead. The framework allows detectors to exchange evidences only when necessary. On-Demand Secure Byzantine Resilience (ODSBR) routing protocol [7],which provides resilience to Byzantine attacks caused by individual or colluding nodes. Byzantine attack is nothing but a compromised intermediate nodes work in collision carries out some of the attacks such as creating loops, routing packets to non optimal paths, selectively dropping packets . Byzantine attack is hard to detect. ODSBR routing protocol uses a technique called adaptive probing which detects a malicious link after a log n faults have occurred. Problematic links are avoided by using a route discovery mechanism which may relies on a new metric that captures adversarial behavior. ODSBR protocol never partitions the network and reduces the damage caused by attackers.

Behavior Base Anomaly Detection technique [8], which is used to mitigate the routing misbehaviours in MANET. Basic idea of this technique involves Negative Selection Algorithm (NSA).Here Detectors are capable of differentiating well behaving nodes from the misbehaving nodes with perfect accuracy. False Positives can be minimized to good extent but, there may exist some False Negatives due to the differentiation between good behavior and bad behavior of nodes. Adaptive reputation management system [9],which realizes, if there is occurring any changes in node behavior due to changes in network conditions. In this system, time slotted approach is introduced to quickly and accurately captures the changes in node behavior and then showed how detection function can be utilized by Sequential Probability Ratio Test for differentiating normal node behavior and misbehaving node behavior. Mechanism Design Based Secure Leader Election Model for Intrusion Detection System [10], which balances resource consumption among all nodes and prolongs the life time of MANET. Here nodes with most remaining resources has to be elected as leaders, some nodes may behave selfishly to get elected as a leader, to overcome this issues of selfish node, nodes which behave honestly are given incentives in the form of reputation and nodes which are misbehaving with in network are punished.

III. RISK AWARE RESPONSE MECHANISM

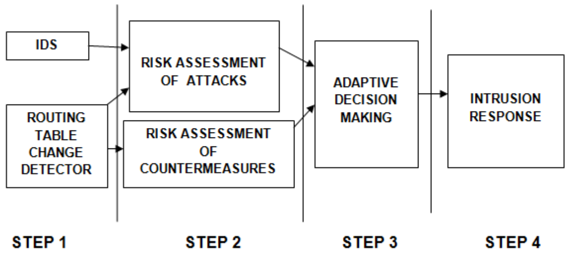
IDS
ROUTING TABLE CHANGE DETECTOR
RISK ASSESSMENT OF ATTACKS
RISK ASSESSMENT OF COUNTERMEASURES
ADAPTIVE DECISION MAKING
INTRUSION RESPONSE
STEP 1
STEP 2
STEP 3
STEP 4

Fig 1: Risk Aware Response Mechanism

To systematically cope up with routing attacks Risk Aware Response Mechanism [11], is used. There are normally four steps in Risk Aware Response Mechanism. They are Intrusion Detection System along with routing table change detector, risk assessment, Adaptative Decision Making and Intrusion Response. Intrusion Detection system gives an attack alert with a confidence value if it finds any misbehaving nodes and Routing Table Change Detector detects all the changes that are occurring in routing table.

The result from intrusion Detection System is taken as an input and entire risk of attack and countermeasures are calculated in Risk Assessment phase using Extended Dempster Shafer Theory. Based on the risk of attack and countermeasures decision is made about whether temporary isolation of node is needed or not in Adaptative Decision making phase .Intrusion Response is made based on the decision.

IV. PROBLEM DESCRIPTION

In Risk Aware Response Mechanism, Intrusion Detection System makes use of static based decision making approach that is , network administrator maintains a profile containing rule set about node threshold value. If the Intrusion Detection System detects any nodes having varying behaviour when comparing the specified rule set created by network administrator, it is considered as misbehaving node or malicious node.

As new attacks are emerging with in MANETs, the network administrator has to update the rule set based upon the new attacks and it's a issue in MANETs and Static Decision Making Approach does not achieve full security with in MANETs.

V. PROPOSED AUTHORIZATION ENFORCEMENT FACILITY AND EXPERIMENTAL SETUP

The experiment is carried out in QUALNET simulator and OLSR protocol is considered for entire simulation. By using AEF how far secure communication takes place between source and destination is analysed with out any malicious activities.

A. Dynamic Access Control Architecture

Normally with in Mobile Adhoc Networks, secure communication can take place only when there are no malicious nodes. If any malicious node is occurring within the network means, its throughput gets affected and high security cannot be achieved. As static based approach is not feasible for achieving full security; Dynamic based approach is combined in these architecture to determine whether source node is a threat or not based on the dynamic conditions in the network.

Dynamic approach [12],would use risk as an input to adapt itself for varying network conditions. Risk refers to how much or how little a source node could be trusted. The main aim is to build a security architecture that uses dynamic access control scheme to perform risk aware network security management.

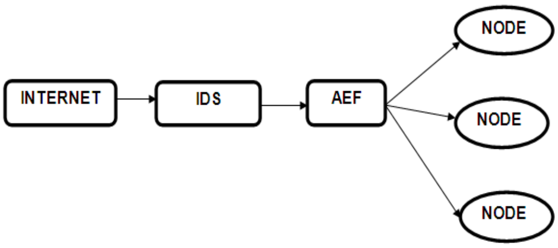

Fig 2 : Conceptual View of Network

Authorization Enforcement Facility (AEF)[12], is mainly used for policy enforcement and enables risk aware network access management. AEF analyses incoming traffic and determines the amount of risk associated with each source. Access from source to destination is allowed only when the risk is low , if the risk is high then access would be denied to destination and on the other hand it performs authorization. The node which needs to transmit data packet has to pass through AEF for authorization.

B. Elements

The elements used in the architecture are given below:

1) *nodes and services:* Using risk aware access management, network can be protected from various malicious nodes by considering some of the assets and those assets are nodes and services, these assets has to be protected. Here node refers to particular machine or device in the network and service refers to the network and internet services provided by the node. Node and services acts as a destination for incoming traffic.
2) *node value and service value:* A node value is a measurable quantity, which states about how valuable the nodes in the network are. Each service can be assigned a service value which states about how valuable the service is .Service value is normally dependent on node value.
3) *roles:* Usually by using role the node value and the service value are kept in track instead of permissions. The role consist of four parts as name, node value, service value, service offered by the node.
4) *threat level:*To determine the risk associated with each source, there must be available some risk and they may be available in the form of quantifiable measure. The quantifiable measure associated here is threat level. Threat level indicates how malicious the source nodes are. Threat level can be specified using threatLevel () function and it returns the threat level of source
5) *thresholds:* Each service value and node value is associated with threshold and this threshold represents the tolerance of a node or services if some suspicious event or action takes place. Threat level keeps on changing dynamically based on the events.
6) *action:* Threat level keeps on changing based on the events. The operation that actually changes the threat level is Action. Action is used for two purposes, first purpose is to adjust the threat level and second, to act as a countermeasure that is triggered as a result of event. New threat level can be calculated based on the previous threat level.

7) *notation:* Notation is used to describe the elements in the architecture

N is a set of nodes $\{n_1 \ldots . n_i\}$
S is a set of services$\{s_1 \ldots s_i\}$
V is a set of node values$\{ v_{1\ldots.} v_k\}$
W is a set of service values$\{ w_{1\ldots} w_k\}$
R is a set of roles $\{r_{1\ldots.} r_m\}$
A is a set of actions $\{a_1 \ldots a_k\}$

Her e the various notation are used to describe the architecture as follows

Services(i) which returns the set of services for node i
role(i) which returns the role of node i
roleservices (m) which returns the services of role m.
nodeservices (i) which returns the services of node i equivalent to role roleservices(role(i)).
nodevalue(i) which returns the node value of node i.
servicevalue(i,j) which returns the service value of service j on node i.
nodeThreshold(i) which returns the threshold of node iserviceThreshold(i,j) which returns the threshold of service j on node i
nvThreshold(v) which returns the threshold of node value V
svThreshold(w) which returns the threshold of service value w.
nodes() which returns all the nodes from $n_{1\ldots.} n_{i.}$
nodeActions(i) which returns all actions of node i.
threatLevel (i) which returns the threat level of source i.

C. *Policy Specification*

The policy specification is subdivided into two sub policies: static policy and dynamic policy. Static policy does not change and while dynamic policy gets changed often.

1) Static Policy: The static policy is specified by the administrator. The static policy is like a regular policy and it does not change until some modification is done on the policy, those modifications can be done only by the administrator .Static policy consist of six sub policies. First, constraints are needed to ensure whether the semantics of the policy are correct. Second, roles which manages and reduces the complexity of assigning node values and service values to many nodes.

   Third, node role assignment which specifies how the roles are assigned to nodes. Fourth, threshold table which defines thresholds for node value and service values. Fifth is the services , which is specified by using file with same format. Sixth is Action which makes use of some arguments they are cost, name, pattern, traffic. Based on this arguments appropriate action would be performed.
2) Dynamic Policy: Dynamic policy is utilized by the system, they keep on changing based on dynamic conditions and simple when compared with static policy. It consists of two column table which keeps track of each source node and current threat level for the specific source.

D. *Policy Enforcement*

In this section, inner working of AEF is described in Figure 3.It is important to understand the relationship between policy enforcement and policy specification .This relationship is illustrated by the way in which the static policy is used by the dynamic policy. When AEF loads the static policy, all the sub policies like constraints ,roles, node role assignments, thresholds, services and actions which are under static policy will be loaded .Based on sub policy information ,nodes are assigned roles, and specified threshold is given for both node and thresholds. The node role mapping and threshold table are kept in internal memory.

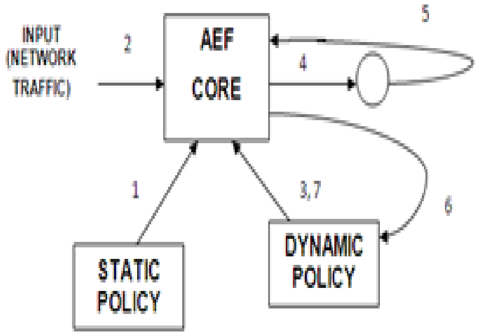

Fig 3: Internal Working of AEF

1) Load static policy
2) Reads and analyze network traffic
3) Initialize and load dynamic policy
4) If granted forward traffic to node
5) Send feedback to aef from node enforcement agentupdate dynamic policy from feedback received
6) Reload dynamic policy

Threat level table in the dynamic policy also gets initialized by the AEF and initial threat levels to all sources are assigned to minimum. Policy Enforcement should perform in such a way that when new source enter into the network, the AEF would examine the arriving nodes and see whether they match any patterns defined by the actions in the policy specification, if the patterns gets matched then the action would increase the threat level. When the threat level increases beyond the threshold value allowed by the static policy then access would be denied otherwise access would be allowed in other case. Hence, only secure communication takes place between source and destination with out any malicious activities achieving higher security in MANETs

VI. PARAMETERS FOR EVALUATION

The parameters that are considered for evaluation are

- Packet Delivery Ratio
- Routing cost
- Packet overhead and byte overhead
- Throughput

Here packet delivery ratio describes about the ratio of total number of packets sent from source and total number of packets received at the destination. Routing cost is the ratio between total bytes of routing packets sent during simulation and total bytes of packets received at the destination. The number of transmitted routing packets is the packet overhead. The number of transmitted bytes by routing packets is the byte overhead.

Fig 4 illustrates the throughput from client in the presence of malicious node ,here warmhole attack property is set to a node and throughput is analyzed using qualnet simulation. Here OLSR protocol is considered for entire simulation

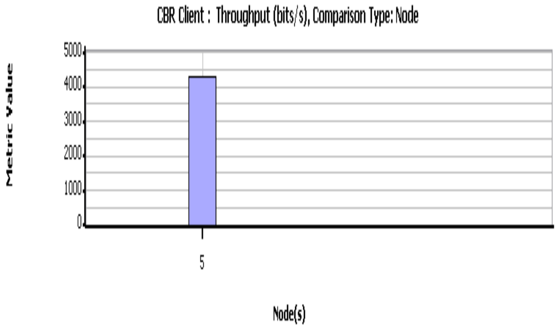

Fig 4: Throughput for client in the presence of warmhole attack

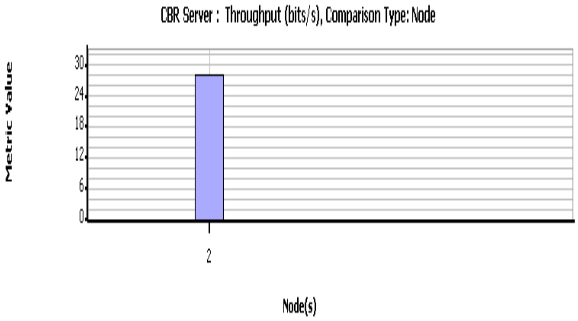

Fig 5: Throughput for server in the presence of warmhole attack

VII. CONCLUSIONS

Intrusion Detection System may sometimes allow malicious nodes to interact within the network for transferring data between sources to destination and hence complete security could not be achieved within the network due to the presence of malicious nodes.Inorder to provide more secure communication between source and destination, Authorization Enforcement Facility is used. AEF uses risk as an input to determine how much source node can be trusted, so that only trusted nodes are allowed to communicate and hence high security can be achieved within MANET.

REFERENCES

[1] Agrawal D., Deng H . and Li W. (2002),' Routing Security in Wireless Adhoc Networks', Proceedings on IEEE Communication Magazine , Vol . 40 , PP. 70-75.

[2] Awerbuch B., Carmela R. Holmer D. Nita-Rotaru C. and Rubens H. (2008) ' ODSBR : An On- Demand Secure Byzantine Resilient Routing Protocol for Wireless Adhoc Networks', proceedings in ACM Transactions of Information System Security, Vol.10, pp. 1- 35.

[3] Felix J., Joseph C. Lee B.S. Das A. Seet B. (2011), 'Cross-Layer Detection of Sinking Behavior in Wireless Adhoc Networks using SVM and FDA', IEEE Transaction in Dependable and Secure Computing, Vol.8 , pp.233-235.

[4] Hu Y., Johnson D. and Perrig A. (2003) , 'SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks ',Adhoc Networks, Vol.1, pp. 175-192.

[5] Hu Y., Perrig A. and Johnson D. (2005) , 'Ariadne : A Secure On- Demand Routing Protocol for Ad Hoc Networks' , Wireless Networks, Vol. 11,pp. 21-38.

[6] Kannhavong B., Nakayama H. Nemoto Y. Kato N. and Jamalipour A. (2007) , ' A Survey of Routing Attacks in Mobile Ad Hoc Networks', Wireless Communication Magazine, Vol. 14, pp. 85-91.

[7] Karlof C., and Wagner D. (2003),' Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures' , Ad Hoc Networks,vol.1 , pp. 293-315.

[8] Levine B., Shields C. and Belding-Royer E. (2002) , 'A Secure Routing Protocol for Ad Hoc Networks', Proceedings on 10th IEEE International Conference Network Protocols , pp. 78-88.

[9] Mohammed N., Otrok H. Wang L. Debbabi M. and Bhattacharya P.2011) , 'Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET' IEEE Transaction , Dependable and Secure Computing , Vol. 8, pp. 89-103.

[10] Marti S., Giuli T. Lai K. and Baker M. (2000),'Mitigating Routing Misbehavior in Mobile Ad Hoc Networks', Proceedings of ACM Mobile Communication, pp. 255-265.

[11] Refaei M., DaSilva L. Eltoweissy M. and Nadeem T. (2010), Adaptation of Reputation Management Systems to Dynamic Network Conditions i n AdHoc Networks', vol. 59,pp. 707-719.

[12] Teo L., Ahn G. and Zheng Y.(2003), 'Dynamic and Risk – Aware Network Access Management', Proceedings of Eighth ACM Symposium ,Access Control Models an Technologies , pp. 217-230.

[13] Tseng C., Wang S. Ko C. and Levitt K.(2006),'DEMEM : Distribute Evidence Driven Message Exchange Intrusion Detection Model For ManetProceedings on 9 th international Symposium, Recent Advances in Intrusion Detection , pp. 249-271.