ISOLATION OF CLONE NODES AND BLACKHOLE NODES USING RISK AWARE MITIGATION

Mebi Sernaz*1, Anand Pavithran*2

*1M.Tech Student & Computer Science Department & Calicut University
*2MES College of Engineering, Kuttippuram, Kerala, India

Abstract— Mobile Ad hoc Networks (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. MANET is distinguished from other networks mainly by its self configuring and optimizing nature. Being the flexible network, MANET is exposed to various kinds of attacks especially the routing attacks. Attack prevention methods such as intrusion detection system, intrusion prevention, authentication and encryption can be used in defense for reducing certain attack possibilities. Intrusion detection system monitors and analyses the activities of the nodes and determines the performance with the security rules. An intrusion Response System will take further actions on recovering the affected services and reconfigure the system. Due to the continuous change in topology and an open vulnerable media network, achieving security in ad hoc networks is very difficult.

Keywords— Black hole attack, MANET, Node replication attack, Risk awareness, Time and space domain detection.

I. INTRODUCTION

MANET is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Each node participating in the network acts both as host and a router. MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. There exist many intrusion response mechanisms for routing attacks.

A. Node replication attack

Node replication attack [6] is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network. Mobile Ad Hoc Networks are highly vulnerable to intrusion, node compromise and physical capture attacks since they are not protected by tamper-resistant hardware due to their low-cost and small size. If captured, the devices can be easily compromised and cloned. The cloned devices will have the same identity as legitimate devices and interact with other devices in the network. One of the major threats is that these cloned nodes can be used to launch several insider attacks, take over the entire network and cause severe destruction. Due to mobility, cloned node collusions and large number of compromised nodes, these attacks are not easily detectable.

B. Black hole attack

In this attack [7], malicious nodes trick all their neighbouring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighbouring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighbouring node, in the black hole attacks, only one attacker is involved and it threatens all its neighbouring nodes.

II. LITERATURE SURVEY

The first response method for intrusion was based on cooperation and trust evaluation was proposed by Sun et al [1]. In this method it quantitatively measure trust and model trust propagation in ad hoc networks. Trust values are associated with two actions: forwarding packets and getting recommendations. Each node in a network maintains a trust record, a recommendation buffer and an observation buffer. For obtaining trust recommendation, a node checks its trust record and selects a set of trusted nodes. The node finds the trustworthiness of the route nodes from its own Trust record or by Requesting Recommendation. Once the node finds the trustworthy route it will update the trust record based on the observation of route quality. This can cause traffic overhead and
delay due to the establishment of trust recommendation. To reduce overhead TRR message will consist of Time To Live (TTL). Dynamic Source Routing (DSR) is used as the underlying routing protocol. A distributed scheme is designed in [1] to acquire, maintain, and update trust records associated with the behaviors of nodes’ forwarding packets and the behaviors of making recommendations about other nodes. The advantages are malicious nodes can be detected and types of malicious behavior can be identified, with the trust recommendations and trust records the presence of malicious nodes in the route can be mitigated.

Reputation management systems proposed by Refaei et al [2] are a cooperation enforcement solution in ad hoc networks. In this Sequential Probability Ratio Test (SPRT) is used to distinguish between cooperative and malicious neighbors. The node behavior may vary from one node to another and from time to time due to changes in local and network-wide conditions, affecting the ability of the reputation management mechanism to distinguish between a node’s willful decision not to forward packets and its inability to do so due to adverse network conditions. Refaei et al [2] evaluated the node behavior in a time slot manner with slot varying according to the congestion and channel impairment.

Refaei et al [2] considers the selfish misbehavior node. The behavior evaluation uses packet forwarding as the metric to evaluate the node behavior. Each node requires localized observations like packet forwarding request events, packet forwarding events and packet dropping events (denoted as RCV, FWD and DRP events) that reflect their neighbors’ behavior. This requires each node to act in promiscuous mode and distinguish data packets that reflect RCV or FWD events related to its neighbors. Each node then stores packet traces for data packets that reflect an RCV event in a lookup table in order to identify any subsequent FWD events. Each RCV event in the lookup table will have a time-out associated with it. If an FWD event is not noted within the duration of that time-out, a DRP event is triggered and the corresponding RCV event entry in the lookup table is purged. This process results in computation and storage overhead.

ADRS proposed by Wang et al [3] plays a vital role in analyzing the anomalous events in MANET. ADRS analyses the MANET anomalies resulted by both intentional and unintentional attacks. Each Anomaly Detector (AD) in an ADRS monitors the behavior and traffic of the neighboring nodes and shares the information between the other AD’s. The overhead is negligible due to light weight of AD’s. The behavior of the node is determined by the packet forwarding ratio. The major parameter for an ADRS detecting the node behavior is based on a threshold value which it determines the distance between the regularity of monitored events and that of normal profiles. ADRS is evaluated by means of detection accuracy and false positive rate.

But cost of operation that includes detection cost and response cost is ignored. As each network node is autonomous, it may refuse to run an ADRS sensor if the overhead impedes its normal operations. It is a significant issue to explore the tradeoffs between detection performance and operational cost (and other metrics) of an ADRS, so that the best detection performance can be achieved with the minimum operational cost.

A method proposed by Marti et al [4] also provides good intrusion response. They used a technique called Watchdog to identify the malicious or misbehaving nodes in a network topology and pathrater to guide the routing protocols to avoid these detected misbehaving nodes and provide another path. The two techniques are extended to the Dynamic Source Routing (DSR) algorithm to reduce the misbehaving nodes in a network. Watchdog can detect the neighboring node behavior by listening to them, if any node does not forward the packet this will be considered as the misbehaving node. A buffer is maintained, where the recently sent packet is stored and compares each packet overhead with the packet in the buffer to see if there is a match. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends
a message to the source notifying it of the misbehaving node.

Pathrater uses the information from the watchdog to check the misbehaving nodes. It picks the most reliable path for the nodes to communicate. It will have a node rating based on which the path reliability is calculated. When calculating path rates, if all other nodes are neutral nodes the pathrater picks the shortest length path. The pathrater does not modify the ratings of nodes that are not currently in active use. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the percentage of overhead transmission from 12% to 24%.

One of the recent systems was proposed by Zhao et al [5]. This system does not isolate the node but evaluates the node behavior based on the threshold set and decides whether it has to completely isolate or temporarily isolated. The risk aware response mechanism is divided into the following four steps. During evidence collection, IDS gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack. Then Risk assessment is performed. Risk of countermeasures is also calculated during a risk assessment phase. The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner. The response level is additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action. The response action and band boundaries are all determined in accordance with risk tolerance and can be changed when risk tolerance threshold changes.

Xing et al [6] proposed a method for detecting clone nodes using the time and location of the collusion of nodes. TDD and SDD provide high detection accuracy and excellent resilience against smart and colluding replicas, have no restriction on the number and distribution of replicas, and incur low communication/computation overhead. TDD and SDD are the only approaches that support mobile networks while place no restrictions on the number and distribution of the cloned frauds and on whether the replicas collude or not. It forces the replicas in MANETs to keep on generating paradoxes along their movements and when they communicate. By looking up these paradoxes, it can detect the replicas at a very high accuracy. It explore the simple one-way hash function for replica attack detection, which results in low computation overhead. SDD scheme is a purely localized scheme that produces low communication overhead. It makes no assumption on the underlying mobility model. Therefore they are applicable to a wide range of mobile networks.

III. PROPOSED SYSTEM

Risk aware mitigation provides better response with adaptive isolation and the response cost calculation when IDS inform it with an alert confidence value. Clone detection based on TDD and SDD provide high detection accuracy and excellent resilience against smart and colluding replicas with low communication overhead. By combining TDD and SDD with risk aware mitigation, a good detection and response mechanism can be developed for the detection of clone nodes in MANET.

Whenever two nodes meet each other both will exchange some information such as time & location at when and where they meet each other. Information exchange process should happen with all nodes the node meets on the way. If anyone fails, from the knowledge of the neighborhood node can easily detect the abnormal silence of the replica node. They also exchange challenge key which contains least and unused index of the node. With this technique can easily detect an attacker node by detecting its location. The main advantages are:

1) No restriction in the detection of number and distribution of replicas.
2) Improve detection accuracy disregarding node collusion.
3) Reduce network damage.
The routing protocol implemented here for mobile nodes are Adhoc On-demand Distance Vector Routing Protocol, which is more prone to black hole attack. Since it is using AODV protocol, it is an efficient energy model which helps to reduce the energy of the system. AODV has borrowed the concept of destination sequence number to maintain the most recent routing information between nodes. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

Since replicated nodes have all legitimate security credentials they can launch various insider attacks, or even take over the network easily. Here the clone node is launching a black hole attack. So the attack model has been implemented and a good response system is provided with risk aware mitigation. By considering the routing table changes the attack node is isolated adaptively.

IV. SIMULATION DETAILS

The project is simulated using NS-2.29 with Linux background simulator. A simulation area of 750*750 has been created and consists of 46 AODV mobile nodes. Packets among the nodes are transmitted with constant bit rate (CBR) of one packet per second. All the needed parameters for the nodes have been defined at the beginning of simulation. Each node has been assigned with an unique ID. The project implementation includes the following modules:

A. Creation of MANET  
B. Route discovery  
C. Implementation of AODV Protocol  
D. Creating the risk aware  
E. Performance analysis

A. Manet Creation  

MANET scenarios in a topology of X*Y meters area. The total simulation time was set into 150seconds, and the bandwidth was set to 2 Mbps. Constant Bit Rate (CBR) traffic was used to send 512 byte-UDP packets between nodes. The queuing capacity of every node was set to 15. We adopted a random traffic generator in the simulation that chose random pairs of nodes and sent packets between them. Every node kept track of all packets sent by it and the entire packet received from other nodes in the network.

B. Route Discovery  

A source node send a broadcast message to its neighbouring nodes if no route is available for the desired destination containing source address, source sequence number, destination address, destination sequence number, broadcast ID and hop count. Two pointers such as forward pointer and backward pointer are used during route discovery. Forward pointers keep track of the intermediate nodes while message being forwarded to destination node.

Eventually, when route request message reached the destination node, it then unicasts the reply message to the source via the intermediate nodes and the backward pointer keeps track of the nodes. It’s to perform route discovery, the source node broadcasts a route request packet with a recorded source route listing only itself. Each node that hears the route request forwards the request (if appropriate), adding its own address to the recorded source route in the packet. The route request packet propagates hop-by-hop outward from the source node until either the destination node is found or until another node is found that can supply a route to the target. The major feature of AODV that distinguish it from DSR is the destination sequence number which is used to verify the up-to-date path to the destination.

As it is an on-demand routing protocol, so it looks up the routing during transmission of a packet. At the first phase, the transmitting node search its route cache to see whether there is a valid destination exists and if so, then the node starts transmitting to the destination node and the route discovery process end here. If there is no destination address then the node broadcasts the route request packet to reach the destination. When the destination node gets this packet, it returns the learned path to the source node.
The advantages of this protocol are:
1. Aware of existence of alternative paths that helps to find another path in case of node or link failure.
2. It avoids routing loops and less maintenance overhead cost as it an on-demand routing protocol.

On the other side, the disadvantages are:
1. Long route acquisition delay for the route discovery which may not be acceptable in situations like the battle field.
2. It is not suitable for large number of nodes where speed may suffer and
3. It produced huge messaging overhead during busy times

C. Protocol Implementation

The events that must be determined are:

When to initiate a route request: This is indicated by a locally generated packet that needs to be sent to a destination for which a valid route is not known.

When and how to buffer packets during route discovery: During route discovery packets destined for the unknown destination should be queued. If a route is found the packets are be sent.

When to update the lifetime of an active route: This is indicated by a packet being received from, sent to or forwarded to a known destination.

When to generate a RERR if a valid route does not exist: If a data packet is received from another host and there is no known route to the destination, the node must send a RERR so that the previous hops and the source halt transmitting data packets along this invalid route.

When to generate a RERR during daemon restart: After the AODV routing protocol restarts, it must send a RERR message to other nodes attempting to use it as a router. This behaviour is required in order to ensure no routing loops occur.

D. Creating the Risk Aware

The risk-aware response mechanism is based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. In this approach, we use two different responses to deal with different attack methods: routing table recovery and node isolation.

Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET.

Since the attack response actions may cause more damages than attacks, the risks of both attack and response should be estimated. We classify the security states of MANET into two categories: {Secure, Insecure}. In other words, the frame of discernment would be \( \{ \varnothing, \{ \text{Secure} \}, \{ \text{Insecure} \}, \{ \text{Secure}, \text{Insecure} \} \). Then Bel \{ Insecure \} is used to represent the risk of MANET.

1) Selection of Evidences: Our evidence selection approach considers subjective evidence from experts’ knowledge and objective evidence from routing table modification. We propose a unified analysis approach for evaluating the risks of both attack (RiskA) and countermeasure (RiskC).

2) Combination of Evidences: For simplicity, we call the combined evidence for attack, \( E_A \) and the combined evidence for countermeasure, \( E_C \). Thus, BelA (Insecure) and BelC (Insecure) represent risks of attack (RiskA) and countermeasures (RiskC), respectively.

Let us focus on the performance of this routing protocol. We evaluated the performance using ns2. We will analyse packet delivery ratio, packet overhead, routing cost, byte overhead and mean latency. Thus this analysis is the comparison between the existing and proposed system which is a graphical representation.

V. PERFORMANCE ANALYSIS

The performance evaluation is measured by the graphs.

A. Packet delivery ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. This metric shows the reliability of data packet delivery. In figure 1, PDR is plotted against the number of nodes.
B. Packet overhead: The number of transmitted routing packets. For example, a HELLO or TC message sent over four hops would be counted as four packets in this metric. In figure 2, packet overhead has been plotted against number of nodes.

C. Byte overhead: The number of transmitted bytes by routing packets, counting each hop similar to Packet Overhead. In figure 3, byte overhead has been plotted against number of nodes.

D. Routing cost: The ratio between the total bytes of routing packets transmitted during the simulation and the total bytes of packets received by the CBR sink at the final destination. In figure 4, routing cost is plotted against number of nodes.

E. Mean latency: The average time elapsed from “when a data packet is first sent” to “when it is first received at its destination”. In figure 5, mean latency has been plotted against number of nodes.

VI. CONCLUSION

MANET is the combination of peer-to-peer techniques, wireless communications, and mobile computing, provides convenient infrastructure-less communications and could be very useful to provide communications for many applications especially when the infrastructure networks is not feasible. MANETs are highly susceptible to physical capture and/or node compromise attacks. As a consequence of this, attackers can launch node clone attack in which an attacker can deploy several cloned nodes in the network. These clones can become the base of several other attacks.

Intrusion detection system monitors and analyses the activities of the nodes and determines
the performance with the security rules. Once an
IDS finds any irregularities in the performance of a
node, it will generate an alarm alert to the system
administrator for the further actions. Intrusion
Response System will take further actions on
recovering the affected services and reconfigure the
system. Various intrusion response methods have
been developed to detect malicious nodes.

Various methods for the detection and
isolation of misbehaving nodes have been studied.
Each method has its own merits and demerits. By
analyzing the various methods it is clear that the
risk aware mitigation is efficient as it provides
adaptive isolation with response cost analysis.
Implemented an AODV Black hole attack model
and provided a good response with risk aware
mitigation. Since it is an energy efficient model it
reduces the energy of the system. Incorporating
TDD and SDD based clone detection with risk
mitigation helps to provide a better response system
since it consider both adaptive isolation and
response cost.

REFERENCES

Hoc Networks Routing Protocols”, in Proceedings of 5th Annual
Postgraduate Symposium on the Convergence of Telecommunications,
[3]. Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, “Black
hole attack in mobile adhoc networks”, in Proceedings of the 42nd
annual Southeast regional conference , ACM-SE 42, pp. 96-97, New
York, NY, USA, 2004. ACM.
of Trust Modeling and Evaluation for Ad Hoc Network”, IEEE J.
[5]. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, “Adaptation of
Reputation Management Systems to Dynamic Network Conditions in
May 2010.
[6]. S. Wang, C. Tseng, K. Levitt, and M. Bishop, “Cost-Sensitive Intrusion
Responses for Mobile Ad Hoc Networks”, Proc. 10th Int’lSymp. Recent
[8]. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu, “Risk-
Aware Mitigation for MANET Routing Attacks”, IEEE Transactions On
Dependable And Secure Computing, vol. 9, no. 2, March/April
2012.
[9]. K. Xing and X. Cheng, “From Time Domain to Space Domain:
Detecting Replica Attacks in Mobile Ad Hoc Networks” IEEE