Routing Information Recovery with Risk Assessment of Attacks Using Intrusion Detection System In MANET

Hemant D. Sonawane, Vivek D. Badgujar, Devdatta B. Bagul

Abstract— **An ad hoc network is a group of mobile nodes without requiring a centralized administration or a fixed network infrastructure. Due to their distributed nature, ad hoc networks are vulnerable to various attacks. One strategy to improve security of ad hoc networks is to develop mechanisms that allow a node to evaluate trustworthiness of other nodes. However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. The proposed system focus on updating and recovering of router information with risk assessment over various attacks using intrusion detection system in MANET.**

***Index Terms*— IDS, Risk Assessment, MANET.**

I. INTRODUCTION

MANETs are nothing but the networks with unstable locations. Because of remote location requirements they cannot register to a single or dedicated router computer which in result makes it distributed in nature. Distributed nature makes it loosely coupled and add more independence to it apart from it on another coincide it may divide them into partitions due to no administrative controls and observations. The routers are also a remote device in the particular era determined dynamically and has a responsibility to transmit the routing tables by using protocol OLSR (Optimized Link State Routing). Similar and built up on AODV (Ad hoc On-Demand Distance Vector). As stated earlier as these devices may be a cell phone that's why protocol and other routing details should be minimal because processing power should be taken into account. Security is an important issue in the integrated MANET-Internet environment because in this environment we have to consider the attacks on Internet connectivity and also on the ad hoc routing protocols. The focus of this work is on different types of attacks on integrated MANET-Internet communication. We consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. The main advantage of location prediction is to allocate, in advance, the convenient next access point before the mobile terminal leaves its current one, in order to reduce the interruption time in communication between terminal mobiles. In without infrastructure networks or MANETs, mobile's location means its geographic coordinates. Location prediction in Ad Hoc networks is a new topic. Its main advantage is to estimate link expiration time in order to improve routing performances.

Manuscript received December 23, 2014.
Hemant D. Sonawane, hd.sonawane@gmail.com
Vivek D. Badgujar, badgujarvivek83@gmail.com
Devdatta B. Bagul, devdatta.bagul14@gmail.com

- **Routing Attacks:**
- Routing Table Overflow
- Routing Table Poisoning
- Packet Replication
- Route Cache Poisoning
- Rushing Attack

II. EXISTING SYSTEM

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses. However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning.

III. PROPOSED SYSTEM

The system address the problem of jamming under an internal threat model and consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

IV. PROPOSED METHODOLOGY

a. Create Network
- Fetching IPs from connected network.
- Creating pairs of IP and ID.

b. Configure Network
- Declare Admin node.
- Create links between nodes.
- Communicate with communication module of another node.
- Send source IP.

- Store source IP, send acknowledgement.

c. IDS-Intrusion Detections System

- Check nodes.
- Find victims.
- Transfer information by passing malicious node.
- Forward to Routing Table Change Network.

d. AODV Protocol

- Reflect changes in table.
- Keep track of number of changes.
- Runs to figure out how many changes on routing table are caused by the attack.

e. Risk Assessment of Attacks

Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Create Confidence value for identification of culprit nodes.

f. Risk Assessment of Countermeasures

Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and\ the risk of countermeasures, the entire risk of an attack could be figured out.

g. Adaptive Decision Making

The adaptive decision module provides a flexible response decision making\ mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

h. Intrusion Response

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.

i. Routing Table Recovery

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

CONCLUSION

The research on MANET security is still in early stage. MANET is easily ulnerable to security attacks then wired network. We have proposed a risk-aware response solution for mitigating MANET routing attacks. Especially, our approach considered the potential damages of attacks and countermeasures. In order to measure the risk of both attacks and countermeasures, we extended Dempster-Shafer theory of evidence with a notion of importance factors. Based on several metrics, we also investigated the performance and practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk aware approach. Based on the promising results obtained through these experiments, early stage we would further seek more systematic way to accommodate node reputation and attack. Frequency in our adaptive decision model.

REFERENCES

[1] Risk aware mitigation for MANET routing attacks. IEEE transactions on dependable and secure computing, vol. 9, no. 2, march/april 2012

[2] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET,” IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.

[3] J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet, “Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA,” IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 233-245, Mar./Apr. 2011.

[4] 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.