IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 4 (April. 2013), ||V2 || PP 08-11

Threat–Attentive Alleviation for Manet Direction-Finding Assaults

N.Venkata Siva Reddy [1],M.Venkata Ramana[2],N.Venkata Krishna[3], P.Obulamma[4]
1, 3, 4. M.Tech students, 2. Assistant Professor
Global College of Engineering & Technology, kadapa

Abstract: Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Even though there exist several intrusion response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. In this paper, we propose a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. 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.

Newer generations of mobile computing equipment come with wireless support standard. In 2003, 55% of laptops sold had embedded wireless support built in, and this percentage is expected to grow even more due to technologies like Intel's Centrino chip. Indeed, from corporate networks to home networks, the number of wireless networks and clients is on the rise. Wi-Fi has undertaken a remarkable journey in the space of just a few short years. D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields, where precise measurement is impossible to obtain or expert elicitation is required. D-S theory has several characteristics. First, it enables us to represent both subjective and objective evidences with basic probability assignment and belief function.

In this paper, we propose a risk-aware response mechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation method. Our risk-aware approach is based on the extended D-S evidence model. In order to evaluate our mechanism, we perform a series of simulated experiments with a proactive MANET routing protocol, Optimized Link State Routing Protocol (OLSR). In addition, we attempt to demonstrate the effectiveness of our solution.

II. BACKGROUND

In this section, we overview the OLSR and routing attacks on OLSR.

2.1 OLSR Protocol

The major task of the routing protocol is to discover the topology to ensure that each node can acquire a recent map of the network to construct routes to its destinations. Several efficient routing protocols have been proposed for MANET. These protocols generally fall into one of two major categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as Ad hoc On Demand Distance Vector (AODV) protocol, nodes find routes only when they must send data to the destination node whose route is unknown. In contrast, in proactive routing protocols, such as OLSR, nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time. OLSR protocol is a variation of the pure Link-state Routing (LSR) protocol and is designed specifically for MANET. OLSR protocol achieves optimization over LSR through the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. Unlike LSR, where every node declares its links and forward messages for their neighbors, only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

Based on the behavior of attackers, attacks against MANET can be classified into passive or active attacks. Attacks can be further categorized as either outsider or insider attacks. With respect to the target, attacks could be also divided into data packet or routing packet attacks. In routing packet attacks, attackers could not only prevent existing paths from being used, but also spoof nonexistent paths to lure data packets to them. Several studies have been carried out on modeling MANET routing attacks. Typical routing attacks include black hole, fabrication, and modification of various fields in routing packets. All these attacks could lead to serious network dysfunctions. In OLSR, any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity. Therefore, the attacker can abuse the properties of the selection algorithm to be selected as MPR. The worst case is the possible selection of the attacker as the only MPR of a node. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation.

III. RISK-AWARE RESPONSE MECHANISM

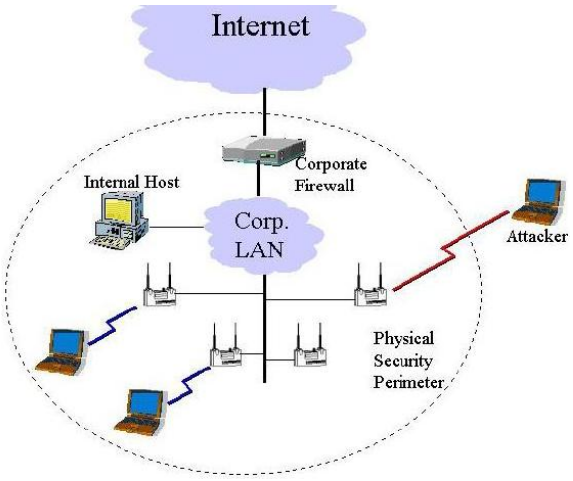
In this section, we articulate an adaptive risk-aware response mechanism based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. We perform risk assessment with the extended.

3.1 Overview

Because of the infrastructure-less architecture of MANET, our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships.

Evidence collection: In this step, Intrusion Detection System (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.

Risk assessment: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. 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.

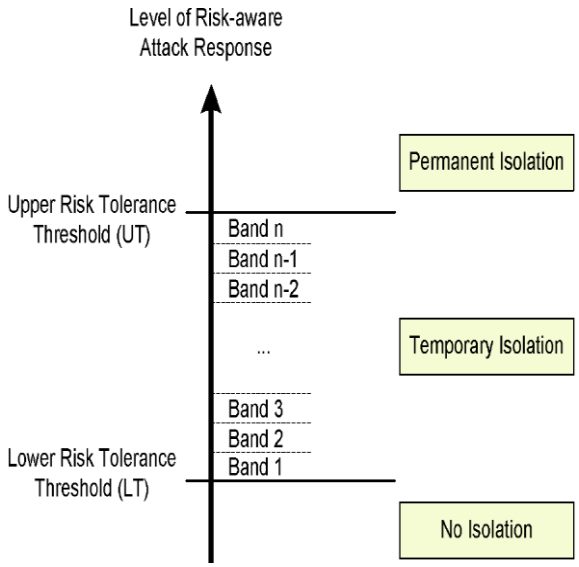


Intrusion response: With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

3.3 Adaptive Decision Making

Our adaptive decision-making module is based on quantitative risk estimation and risk tolerance, which is shown in below diagram. 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. The upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would remain each node intact. The band between the upper tolerance threshold and lower tolerance threshold is associated with the temporary isolation response,

in which the isolation time (T) changes dynamically based on the different response level given by and, where n is the number of bands and i is the corresponding isolation band.



IV. CASE STUDY AND EVALUATION

In this section, we first explain the methodology of our experiments and the metrics considered to evaluate the effectiveness of our approach. Then, we demonstrate the detailed process of our solution with a case study and also compare our risk-aware approach with binary isolation. In addition, we evaluate our solution with five random network topologies considering different size of nodes. The results show the effectiveness and scalability of our approach.

V. METHODS

Importantly, however, the speed of Wi-Fi innovation is replicated at the low end of the market. Wi-Fi has become an integral feature of low-cost devices sold in huge volume in emerging markets. Price-sensitive consumers in markets such as China and India can purchase locally-manufactured devices with Wi-Fi support for less than US$50. But branded devices are also reaching the market at lower and lower price points with Nokia's Asha series of 2G and Wi-Fi-capable devices a key but by no means isolated example. Clearly, the momentum behind Wi-Fi gathered pace during 2012 and the outlook for the coming 12 months is equally positive for the Wi-Fi ecosystem. There are three key factors that will add further fuel to the fire. Security, cost, and convenience may motivate the use of multilevel networks. It reduces the number of separate machines that individual users must log into and also reduces the operational costs of housing all of the extra equipment necessary to run separate networks for each classification level. Multilevel networks also allow the sharing of data across different sensitivity levels in real time.

The association process is a two-step process involving three states:

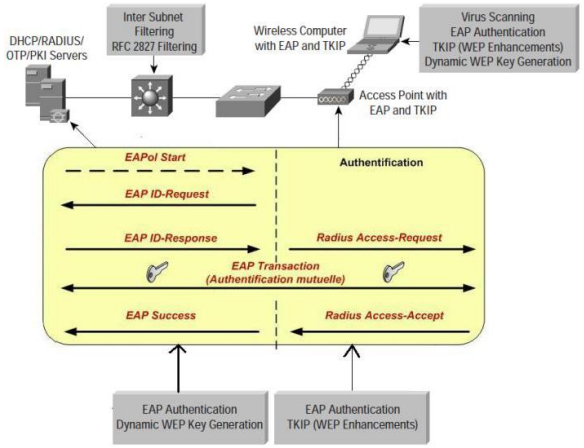
1. Unauthenticated and unassociated,
2. Authenticated and unassociated,
3. Authenticated and associated.

In the below figure, after identifying an access point, the client and the access point perform a mutual authentication by exchanging several management frames as part of the process. The two standardized authentication mechanisms are described. After successful authentication, the client moves into the second state, authenticated and unassociated.

VI. RELATED WORK

Wi-Fi is also appearing in many new devices, not just in laptop and desktop computers. Many PDAs have slots for Wi-Fi cards, and the first Wi-Fi capable phones are appearing on the market. The growth of devices will undoubtedly spur even more innovation in the public wireless LAN marketplace. In ad hoc mode, each client communicates directly with the other clients within the network, the ad hoc mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. When

WLAN data is not encrypted, the packets can be viewed by anyone within radio frequency range. For example, a person with a Linux laptop, a WLAN adapter, and a program such as TCPDUMP can receive, view, and store all packets circulating on a given WLAN.



Risk-aware approaches: When it comes to make response decisions, there always exists inherent uncertainty which leads to unpredictable risk, especially in security and intelligence arena. Risk-aware approaches are introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way.

VII. CONCLUSION

We have proposed a risk-aware response solution for mitigatingMANETrouting 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, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

REFERENCES

[1]. 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.

[2]. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70- 75, Oct. 2002.

[3]. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85- 91, Oct. 2007.

[4]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, 2000.

[5]. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28- 39, May/June 2004.