International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2577-2580 ISSN: 2249-6645

An Optimal Risk- Aware Mechanism for Countering Routing Attacks in MANETs

Shaik Silarbi[1], G. Sridevi[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India*
[2]*Assoc. Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India*

***Abstract*:** *Mobile Ad Hoc Networks (MANET) are a distributed and self configuring wireless networks. MANETs does not have a predefined network infrastructure. Application of MANET is benefited in areas such as disaster relief, military services and mine site operations. Each node communicates with the other acting nodes as routers. The co-operation and trust between the nodes are depended for the proper functioning of MANET. Being the flexible network, MANET is exposed to various types of attacks especially the routing attacks. There are various methods introduced to mitigate such critical routing attacks. In this paper, we propose a risk-aware response mechanism to systematically cope with the routing attacks in MANET, proposing an adaptive time-wise isolation method. Our risk-aware approach is based on the extended Dempster-Shafer (D-S) evidence model. D-S theory has been adopted as a valuable tool for evaluating the reliability and security in information systems and by other engineering fields, where precise measurement is impossible to obtain or expert elicitation is required.*

Keywords: *D- S theory, MANET, Routing attack.*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET)[1] (Figure 1) is distributed and self configuring wireless network. MANETs does not have a predefined network infrastructure. Application of MANET is benefited in areas such as disaster relief, military services and mine site operations. Each node communicates with the other nodes acting as routers. The co-operation and trust between the nodes are depended for the proper functioning of MANET. Since the network topology in MANET changes unpredictably and rapidly it is highly vulnerable to various types of attacks. Attack prevention methods such as authentication and encryption, intrusion detection system, intrusion prevention can be used in defense for reducing certain attack possibilities. MANET is considered one of the most promising fields in both research and development of wireless networks. There exist many intrusion response mechanisms for the routing attacks. The existing techniques usually attempt to isolate the vulnerable nodes from the topology there by causing the partition of network topology.

Methods such as binary responses may result in the unexpected network partition, thereby causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. Several intrusion detection techniques have been introduced for detecting the vulnerable nodes and preventing the neighbor nodes compromised by the malicious nodes. Even though several mechanisms and routing protocols are introduced each of them has one or more vulnerabilities. Research on the MANETs and implementation has become a huge amount of task to be done. When a malicious node is being identified then the node has to be either repaired or another route has to be established. In most of the existing techniques the nodes when found slightly malicious is completely isolated from the entire network which will make splitting of the network and thereby causing communication problems between the nodes.

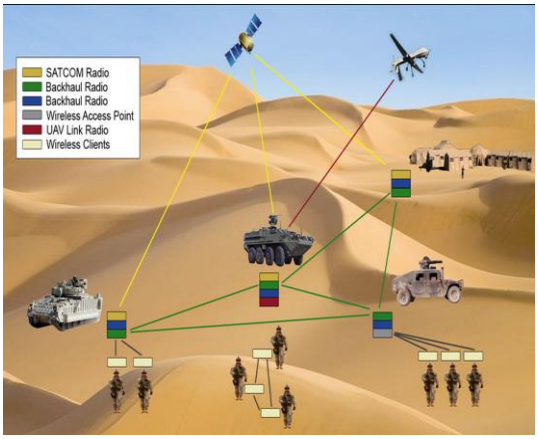

Figure 1: An Example MANET

II. RELATED WORK

In [2], the authors propose the ariadne protocol for preventing the attacks against the networks. An ad hoc network is a group of wireless mobile computers or nodes, in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, thereby assuming a trusted environment. Here routing attacks are

presented against routing in ad hoc networks, and the design and performance evaluation of a new secure on-demand ad hoc network routing protocol is presented i.e. called Ariadne. Ariadne [2] prevents compromised nodes or attackers from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service (DOS) attacks.

In [3], the authors has presented the Secure Efficient Ad hoc Distance vector routing protocol (SEAD) mechanism to guard against the DoS attacks. An ad hoc network is a collection of wireless computers or nodes, communicating among themselves over possibly multi- hop paths, without the help of any infrastructure such as base stations or access points. In [4], the authors proposed a vector model for all security services rely to a great extent on some notion of trust. However, even today, there is no accepted technique or formalism for the specification of trust and for reasoning about trust. In [5], the authors developed an alternative methodology for the risk analysis of information systems security (ISS), an evidential reasoning approach under the Dempster-Shafer theory of belief functions. In [6], the authors has proposed the cooperative enforcement approach. Ad hoc networks rely on the co- operation of the nodes [6] participating in the network to forward packets for each other. A node may decide not to co- operate to save all its resources while still using the network to relay its traffic. If too many nodes exhibit this behaviour, the network performance degrades and cooperating nodes may find themselves unfairly loaded. If a node observes another node that not participating correctly, it reports this observation to other nodes who then take action to avoid being affected and potentially punish the bad node by refusing to forward its traffic.

III. PROPOSED WORK

A. Risk- aware Response Mechanism

In this section, we have a tendency to articulate an adjustive risk-aware response method supported quantitative risk estimation and risk tolerance. Rather than applying easy binary isolation of the malicious nodes, our approach adopts an isolation mechanism in a very temporal manner supported the danger price. We have a tendency to tend to perform risk assessment with the extended D-S proof theory introduced in for every routing attacks and corresponding countermeasures to make extra correct response picks illustrated in Figure 2.

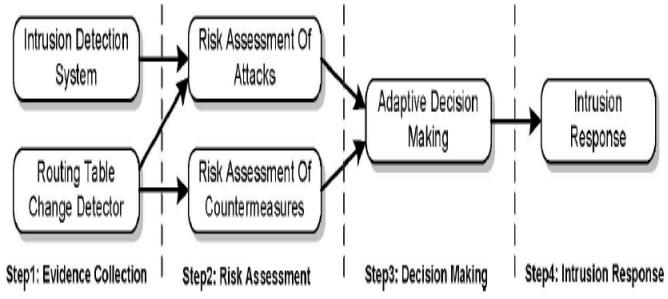

Figure 2: Risk-aware response mechanism

Evident Collection: In this step Intrusion Detection System (IDS) provides associate degree attack alert with a confidence price, and so the routing Table modification Detector (RTCD) runs to work out what percentage changes on routing table area unit caused by the attack.

Risk Evaluation: Alert confidence from IDS and therefore the routing table would be an additional thought-about as freelance evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated moreover throughout the risk assessment section, supported the danger of routing attacks and thus the chance of countermeasures, the whole risk of associate attack is also discovered.

Decision Creating: The accommodative decision module provides a flexible response decision making method, that takes risk estimation and risk tolerance into consideration, to control the temporary isolation level, a user can set fully totally different thresholds to satisfy her goal.

Intrusion Response: With the output from the risk assessment and decision-making module, the corresponding response actions, at the side of the routing table recovery and node isolation, administered to mitigate attack damages throughout a distributed manner.

B. Response to Routing attacks

In this approach, we use two different responses to deal with different attack methods: routing table recovery and the node isolation. Routing table recovery includes the local routing table recovery and global routing recovery. Local routing recovery is performed by the victim nodes that detect the attack and automatically recover its own routing table. Node isolation may be the most intuitive way to prevent further routing attacks from being launched by malicious nodes in MANET. To perform a node isolation response, the neighbors of the malicious nodes ignore the malicious node by neither forwarding packets through it nor accepting any network packets from it. Figure 3 shows an example scenario where nodes 2 to 0 are supposed to go through Nodes 3 and 5. Suppose a malicious node 1 advertises a fake link to node 0 and then it

would also cause all other nodes to update its routing table accordingly. As a result the data from Nodes 2 to 0 travels Node 1 rather than nodes 2 and 4 and Node 1 can manipulate and drop the traffic between Nodes 2 to 0.

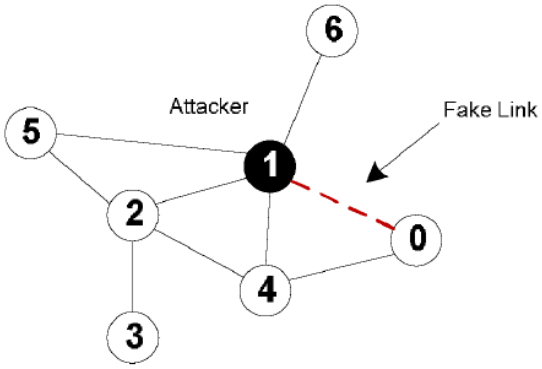

Figure 3: Example scenario

C. Risk Assessment

In risk assessment step, alert confidence from IDS and RTDC would be considered as different evidences and these two evidences combined using Dempster's rule of combination with the importance factors (DRCIF) algorithm. It provides entire risk of attack. Security state of the MANET can be classified into two categories. {Secure, Insecure} which means security state of MANET could be either secure or insecure. Risk of MANET could be represent by belief function called Bel{Insecure}. The algorithm for combination of the multiple evidences is constructed as follows:

Algorithm MUL-EDS-CMB
INPUT: Evidence pool Ep
OUTPUT: One evidence
1 |Ep|= sizeof(Ep);
2 While |Ep| > 1 do
3 Pick two evidences with the least IF in Ep, named E1 and E2;
4 Combine these two evidences,E= <m1 ⊕ m2, (IF1+ IF2)/2>;
5 Remove E1 and E2 from Ep;
6 Add E to Ep;
7 end
8 return the evidence in Ep

D. Adaptive Decision Making

ADM (Adaptive Decision Making) technique is used to provide a flexible response decision making method when it gets attack alert. Our adaptive decision making module is based on the quantitative risk estimation and risk tolerance, which is shown in Figure 4. The response level is additionally splitted into multiple bands. Each band is associated with an isolation degree, which presents a different time interval of the isolation action. The response action and the 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 the permanent isolation response. The lower risk tolerance threshold (LT) will remain each node intact. The band between the upper tolerance threshold and lower tolerance threshold is associated with a temporary isolation response, in which the isolation time "T" changes dynamically based on the different response level given by

$$i = \left\lceil \frac{Risk - LT}{UT - LT} \times n \right\rceil, \; Risk \in (LT, UT)$$

and

$$T = 100 \times i \; (milliseconds)$$

where "n" is the number of bands and i is the corresponding isolation band.

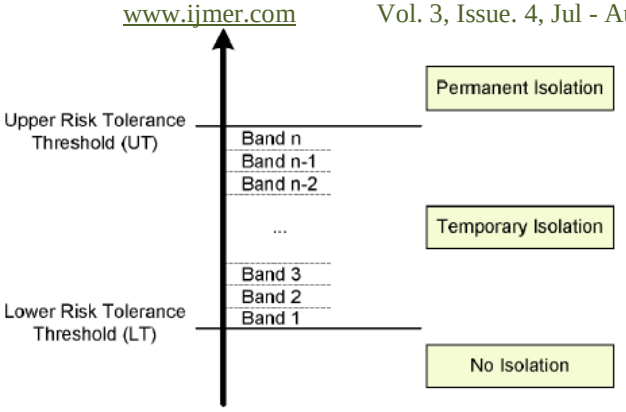

Figure 4: Adaptive decision making

IV. CONCLUSIONS

Mobile ad hoc network (MANET) is a collection of mobile nodes without the required intervention of any existing infrastructure or centralized access point such as a base station. MANET has the dynamic infrastructure hence it is highly vulnerable to various attacks. Several attacks are possible in MANET networks and among them the routing attack could cause the worst damage. There are several solutions available for mitigating such routing attacks. In this paper, we propose an adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and their countermeasures. The adaptiveness of our method allows us to systematically cope with MANET routing attacks.

REFERENCES

[1] 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 (RAIDf'07), pp. 127- 145, 2007.

[2] Hu, Y.C., Perrig, A. and Johnson, D.B. (2002), "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), ACM Press, pp.12–23.

[3] Hu, Y.C., Perrig, A. and Johnson, D.B. (2002), "Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," 4th IEEE Workshop Mobile Computing Systems and Applications (WMCSA'02), pp.3-13.

[4] Ray and Chakraborty, S. (2004). "A vector model of trust for developing trustworthy systems," European Symposium on Research in Computer Security, September, pp. 260–275.

[5] L. Sun, R. Srivastava, and T. Mock (2006), "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.

[6] Bansal, S. and Baker (2003), "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Technical Report cs.NI/0307012, Stanford University, Vol.1, No.2, pp.1-10.