ISSN:0975-9646

Intrusion Determent using Dempster-Shafer Theory in MANET Routing

Karuturi.Satish,
M-Tech Student,
CSE, KITS RCPM

K. Ramesh
Associate Professor,
CSE, KITS, RCPM

Abstract: Mobile Ad Hoc Network (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. Lack of a defined central authority, securitizing the routing process becomes a challenging task in MANETS thereby leaving the network vulnerable to routing attacks, which results in deteriorated network performance thus questioning the reliability of such networks. Prior approaches to mitigate such critical attacks typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. Binary responses may result in the unexpected network partition, giving rise to new anomalies in the network infrastructure, and naïve fuzzy responses could lead to uncertainty in countering routing attacks leading to computation overhead. So we propose a risk-aware response mechanism based on an extended Dumpster-Shafer mathematical theory of evidence that introduces a notion of importance factors to systematically cope with the identified routing attacks. The effectiveness of our approach with respect to several performance metrics is highlighted n the scope of this paper.

Keywords—Mobile ad hoc networks, intrusion response, risk aware, Dempster-Shafer theory.

I INTRODUCTION

Mobile Ad hoc Network (MANET) [1] is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed. MANET are utilized to set up wireless communication in challenging environments without a predefined infrastructure.

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 [2]. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Several work [3], [4] addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET [5].

However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation. Wang et al.[12] proposed a naıve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. In this paper, we seek a way to bridge this gap by using Dempster-Shafer mathematical theory of evidence (D-S theory), which offers an alternative to traditional probability theory for representing uncertainty [13]. D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields [6], [7], 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. Second, it supports Dempster's rule of combination (DRC) to combine several evidences together with probable reasoning. However, as identified in [8], [9], [10], [11], Dempster's rule of combination has several limitations, such

as treating evidences equally without differentiating each evidence and considering priorities among them. To address these limitations in MANET intrusion response scenario, we introduce a new Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model

The chief characteristics and challenges of the MANETs [2] can be classified as follows: Cooperation: If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed. This is known as multi hop communication.

Hence each node is to act as a host as well as a router simultaneously.

Dynamism of Topology:

The nodes of MANET are randomly, frequently and unpredictably mobile within the network.[3] These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes.

Lack of fixed infrastructure:

The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

Resource constraints problem of MANETs usually are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring. Albeit the security requirements (availability, confidentiality, integrity, authentication, non repudiation)[4] remain the same whether be it the fixed networks or MANETs, the MANETs are more susceptible to security attacks than fixed networks due their inherent characteristics.[5] Securitizing the routing process is a particular challenge due to open exposure of wireless channels and nodes to attackers, lack of central agency/infrastructure, dynamic topology etc.[6]. The wireless channels are accessible to all, whether meaningful network users or attackers with malicious intent. The lack of central agency inhibits the classical server based solutions to provide security. The dynamic topology entails that at any time any node whether legitimate or malicious can become a member of the network and disrupt the cooperative communication environment by purposely disobeying the routing protocol rules.

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 the efficiency of our mechanism, we perform a series of simulated experiments with a proactive MANET routing protocol, Optimized Link State Routing Protocol (OLSR) [14].

II RELATED WORK

According to Siaterlis et al. [2003], Siaterlis and Maglaris [2004 and 2005], and Chatzigiannakis et al. [2007] the main disadvantage of the D-S theory is that the assumption it makes that the pieces of evidence is statistically independent from each other. Since sources of information are often linked with some sort of dependence in real life situations, this assumption does not always hold true. Also, in the Siaterlis et al. [2003] framework, they pointed out that the systems inability to detect multiple simultaneous attacks. This was because they assumed a mutually exclusive set of system states.

According to Chen and Aickelin [2006], D-S has two major problems. One they say is the computational complexity associated with D-S. The other is the conflicting beliefs management. According to Chen and Aickelin the computational complexity of D-S increases exponentially with the number of elements in the frame of discernment (Θ). If there are n elements in Θ, there will be up to 2n-1 focal elements for the mass function. Further the combination of two mass functions needs the computation of up to 2n intersections.

Yager [10] and Yamada and Kudo [18] proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. [11] suggested a weighted combination rule to handle the second limitation. However, the weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security and criticality. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations.

Importance factor (IF) is a positive real number associated with the importance of evidence. IFs are derived from historical observations or expert experiences.

Extended DS theory overcomes the above specified limitations

III PRELIMINARIES

ROUTING ATTACKS IN MANET

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail. Here shall highlight some important routing attacks.

3.1 Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network

performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

3.2 Blackhole attack

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

3.3 Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks. An example of the link spoofing attack in an DSR MANET. We assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and E are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbors. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

3.4 Wormhole attack

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual.

3.5 Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and path rater. Consider the case where node A1 forwards routing packets for node T. The first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets.

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. Our risk-aware response mechanism is divided into the following four steps shown in Fig.1 & Fig 2

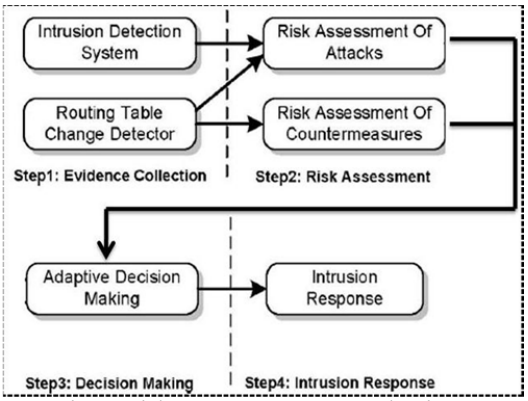

Fig.1: Risk-aware response mechanism.

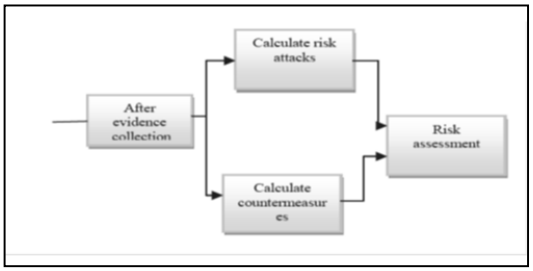

Fig 2: Risk assessment

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.

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 the goal.
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.

IV EXTENDED DEMPSTER-SHAFER THEORY OF EVIDENCE

The Dempster-Shafer mathematical theory of evidence is both a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidences. However, previous research efforts identify several limitations of the Dempster's rule of combination 1. Associative. For DRC, the order of the information in the aggregated evidences does not impact the result. As shown in [13], a non associative combination rule is necessary for many cases. 2. Non weighted. DRC implies that we trust all evidences equally [13]. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence. Yager and Yamada and Kudo proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. [11] suggested a weighted combination rule to handle the second limitation. However, the weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security and criticality. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations.

4.1 Importance Factors and Belief Function In D-S theory, propositions are represented as subsets of a given set. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors.
Definition 1. Importance factor (IF) is a positive real number associated with the importance of evidence. Ifs are derived from historical observations or expert experiences.
Definition 2. An evidence E is a 2-tuple hm; IFi, where m describes the basic probability assignment [13].
Definition 3. Extended D-S evidence model with importance factors: Suppose E1=<m1,IF1> and E2 =< m2, IF2> are two independent evidences. Then, the combination of E1 and E2 is E = <m1 Θ m2,(IF2+IF2)/2>, where Θ is Dempster's rule of combination with importance factors.
Suppose Bel1 and Bel2 are belief functions over the same frame of discernment, with basic probability assignments m1 and m2. The importance factors of these evidences are IF1 and IF2. Then, the function m defined by Our proposed DRCIF is non associative for multiple evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm supports this requirement and the complexity of our algorithm is O(n), where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naıve fuzzy-based method. The algorithm for combination of multiple evidences is constructed as follows:

Algorithm 1. MUL-EDS-CMB

INPUT: Evidence pool Ep

OUTPUT: One evidence
1. jEpj ¼ sizeof(Ep);
2. While jEpj > 1 do
3. Pick two evidences with the least IF in Ep, named E1 and E2;
4. Combine these two evidences, E =<m1 Θ m2, (IF1 + IF2)/2>;
5. Remove E1 and E2 from Ep;
6. Add E to Ep;
7. End
8. Return the evidence in Ep

V PERFORMANCE

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 itself and the entire packet received from other nodes in the network. In order to evaluate the effectiveness of our adaptive risk-aware response solution, we divided the simulation process into three stages and compared the network performance in terms of six metrics. The following describes the activities associated with each stage:
Stage 1—Before attack. Random packets were generated and transmitted among nodes without activating any of them as attackers. This simulation can present the traffic patterns under the normal circumstance.
Stage 2—After attack. Specific nodes were set as attackers which conducted malicious activities for their own profits.However, any detection or response is not available in this stage. This simulation process can present the traffic patterns under the circumstance with malicious activities.
Stage 3—After response. Response decisions for each node were made and carried out based on three different mechanisms.We computed six metrics for each simulation run:
- Packet delivery ratio. The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.
- 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.

- 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.
- Byte overhead. The number of transmitted bytes by routing packets, counting each hop similar to Packet Overhead.
- Mean latency. The average time elapsed from "when a data packet is first sent" to "when it is first received at its destination."
- Average path length. This is the average length of the paths discovered by OLSR. It was calculated by averaging the number of hops taken by each data packet to reach the destination.

Table-1: Communication Overhead due to the presence of Extended DS theory

Protocol	FileSize(bytes)	TransferTime(secs)
OLSR	40960	0.349
OLSR	270336	0.374
OLSR	15454208	1.322

Table-2: Comparison of Three Routing Protocols

Parameters	**AODV**	**DSR**	**OLSR**
Source	No	Yes	No
Routing	Full	Full	Reduced
Topology	Full	Full	Local
Broadcast	Route	Route	Nodes
Update Information	Error	Error	Height
Update Destination	Source	Source	Neighbours
Method	Unicast	Unicast	Broadcast
Storage	O(E)	O(E)	O(Dd*A)

VI CONCLUSION

Derived from the original Dempster-Shafer theory we proposed a risk-aware response solution for handling MANET routing attacks. Our approach considers the potential damages of various attacks and countermeasures. 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 investigated the performance and practicality of our approach interms of effectiveness and scalability with regard various Manet reactive protocols. Based on the established results obtained through our network applicationusage scenario and statistics, we validate OLSR implemented extended DS theory approach has better feasibility ratios in terms of communication and counter measures. We would further seek more systematic way to accommodate node reputation and attack frequency to turn it into an adaptive decision model which can be considered a future research.

REFERENCES

[1] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.

[2] Ziming Zhao, Gail-Joon Ahn. Risk-Aware Mitigation for MANET Routing Attacks, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012

[3] Y. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.

[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.

[5] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy, 2007.

[6] L. Sun, R. Srivastava, and T. Mock, "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, 2006.

[7] 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.

[8] K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.

[9] L. Zadeh, "Review of a Mathematical Theory of Evidence," AI Magazine, vol. 5, no. 3, p. 81, 1984.

[10] R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

[11] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.

[12] 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 (RAID '07), pp. 127-145, 2007.

[13] G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.

[14] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.

AUTHORS PROFILE

Karuturi S R V Satish received B.Tech degree in Information Technologyfrom Lenora College Of Engineering, Rampachodavaram East Godavari District, M.Tech in Computer Science& Engineering . M.Tech in Computer Science& Engineering

Kothapalli Ramesh M.Tech. Associate Professor in Kakinada Institute of Technological Sciences, Ambikapalli Agraharam, Ramachandrapuram(M.L), East Godavari Dist, A.P, India.He has a teaching experience of 9 years.