ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Responsive Risk Analyzing System for MANET Routing Attacks

D.V.Rammohan Reddy[1]
M.Tech Scholar
Department of computer science&Engineering
Sri Sai Madhavi Institute of Science & Technology
Rajanagaram, Rajahmundry
India

Yuvaraju Chinnam[2]
Associate Professor, M.Tech,(Ph.D).
Sri Sai Madhavi Institute of Science & Technology
Rajanagaram, Rajahmundry
India

Abstract: ***Mobile Ad hoc Networks (MANET) which has no central administration 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 intrusions response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, we propose a risk-Analyze Response mechanism to systematically cope with the identified routing attacks. Our risk-analyze approach is based on an extended Demister-Shafer mathematical theory of evidence introducing a notion of importance factors.***

Keywords: Mobile ad hoc networks, intrusion response, malicious, dempster-shafer theory.

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are proven networks but due to its dynamic nature highly affected with attacks. 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 response decisions. These networks 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. 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 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. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET.

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. Proposed a naive 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 project work, 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.

II. Related Work

An Ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. In this paper work we present the solutions based on the following related work.

a) Ad hoc on demand distance vector routing (AODV)

A novel algorithm for the operation of such Ad hoc networks. Each Mobile Host operates as a specialized router and routes are obtained as needed i. e on demand with little or no reliance on periodic advertisements our new routing algorithm is quite suitable for a dynamic self starting network as required by users wishing to utilize Ad hoc networks AODV [1] provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements Nevertheless we can still maintain most of the advantages of basic distance vector routing mechanisms. We show that our algorithm scales to large populations of mobile nodes wishing to form networks. We also include evaluation methodology and simulation results to verify the operation of our algorithm.

The algorithms primary objectives are

1. To broadcast discovery packets only when necessary.
2. To distinguish between local connectivity management neighborhood detection and general topology maintenance.
3. To disseminate information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information.

b) OLSR Routing protocol

The major task of the routing protocol is to construct route to its destinations. Proactive routing protocols OLSR within which nodes get routes by periodic exchange of topology information with other nodes and maintain route information all the time. OLSR protocol [2] achieves optimization through the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. Each node declares its links and forward messages for their neighbors, only nodes selected as MPR nodes are dependable for advertising as well as forwarding an MPR selector list advertised by alternative MPRs .Random packets were generated and transmitted among nodes without activating any of them as attackers. This replication can present the traffic patterns below the traditional Circumstance. In OLSR any node can either modify the protocol messages before forwarding them or generate false messages or spoof an identity. Therefore the aggressor will abuse the properties of the choice algorithm to be selected as MPR. The most terrible case is the possible selection of the aggressor as the only MPR of a node that offer wrong information about the topology of a network (TC message) in order to disturb the routing operation. Specific nodes were set as attackers which conducted malicious activities for their own profits. This simulation process can present the traffic patterns under the circumstance with malicious activities.

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. 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 (MultipointRelay) 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.

c) Trust Modeling and Evaluation for Ad Hoc Networks

The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trust worthiness [3] of other nodes without centralized authorities. We present an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. We interpret trust as a level of uncertainty and the basic understanding of trust is summarized as follows. Trust is a relationship established between two entities for a specific action. In particular, one entity trusts the other entity to perform an action. In this work, the first entity is called the subject; the second entity is called the agent. The notation to describe a trust relationship is {Subject: agent, action}. In proposed trust models First of all, each node in ad hoc network maintains a trust record, a recommendation buffer, and an observation buffer.

d) Dumpster's Rule of Combination with Importance Factors (DRCIF)

It explains about Failure Modes, Effects, and Criticality Analysis; Event Tree Analysis, Fault Tree Analysis, and Reliability Centered Maintenance [5][6] including a tutorial introduction to the Dempster-Shafer Theory[5][8][9], the differences between the Probability and the Dempster -Shafer Theory are discussed widely. The Dempster-Shafer mathematical theory [18] of evidence is both a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dumpster's rule of combination is the procedure to aggregate and summarize a corpus of evidences. However, previous research efforts identify several limitations of the Dumpster's [10][11] rule of combination.

1. Associative: For DRC, the order of the information in the aggregated evidences does not impact the result.
2. Non weighted DRC: implies that we trust all evidences equally.

In D-S theory, propositions are represented as subsets of a given set. Suppose θ is a finite set of states, and let 2^{θ} denote the set of all subsets of θ. D-S theory calls θ, a frame of discernment. 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.

III. NETWORK ARCHITECTURE

The Risk Analyze system is designed with the following prediction of network architecture. Here the attacker can enter into the system to cause vulnerable action to routing paths.

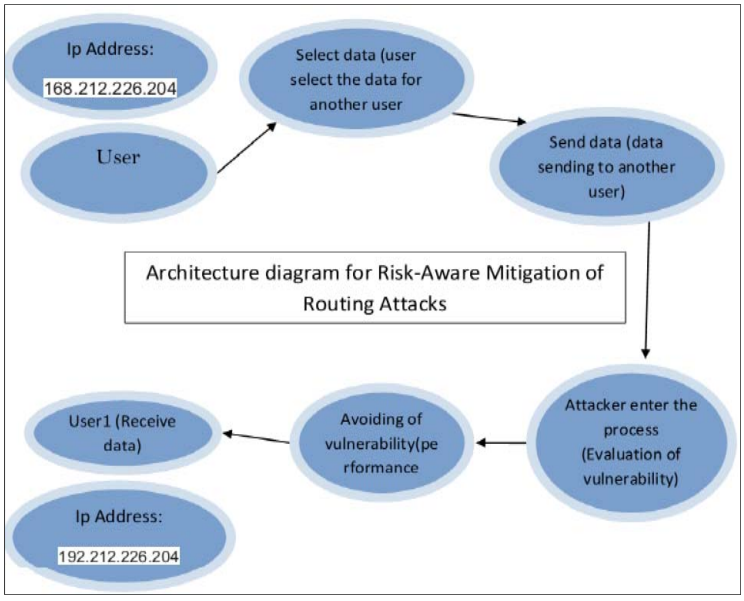

Fig 1.Risk Analyze Network Architecture.

IV. PROBLEM DEFINITION

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. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation. Proposed a naive 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. The disadvantage in this existing system is however, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Dumpster'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 Dumpster's rule of combination with a notion of importance factors (IF) in D-S evidence model.

Most of the work 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.

V. PROPOSED SYSTEM

We formally propose an extended D-S evidence model with importance factors and articulate expected properties for Dempster's rule of combination with importance factors (DRCIF). Our Dempster's rule of combination with importance factors is non associative and weighted, which has not been addressed in the literature. We propose an adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks.

We evaluate our response mechanism against representative attack scenarios and experiments. Our results clearly demonstrate the effectiveness and scalability of our risk- aware approach. In risk aware response mechanism, we articulate an adaptive risk-aware response 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 D-S evidence theory introduced for both attacks and corresponding countermeasures to make more accurate response decisions illustrated. In this project work, 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.The heading of the Acknowledgment section and the References section must not be numbered. Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

There are mainly four phases in the algorithm

Phase 1: Evidence collections phase

Phase 2: Decision making phase

Phase 3: Intrusion response phase

Phase 4: Routing table recovery phase

Phase 1: Evidence collections phase

In 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 (Risk A) and countermeasure (Risk C).We take the confidence level of alerts from IDS as the subjective knowledge in Evidence 1. In terms of objective evidence, we analyze different routing table modification cases. There are three basic items in OLSR routing table (destination, next hop, distance). Thus, routing attack can cause existing routing table entries to be missed, or any item of a routing table entry to be changed. We illustrate the possible cases of routing table change and analyze the degrees of damage in Evidences 2 through 5.

Evidence 1: Alert confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence. Since the false alarm is a serious problem for most IDSs, the confidence factor must be considered for the risk assessment of the attack. The basic probability assignments of Evidence 1 are based on three equations given below:

M (Insecure) = c; c is confidence given by IDS

M (Secure) = 1 - c

M (Secure, Insecure) = 0.

Evidence 2: Missing entry. This evidence indicates the proportion of missing entries in routing table. Link withholding attack or node isolation countermeasure can cause possible deletion of entries from routing table of the node.

Evidence 3: Changing entry I. This evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the malicious node builds a direct link to this node. So, it is highly possible for this node to be the attacker's target. Malicious node could drop all the packages to or from the target node, or it can behave as a normal node and wait for future attack actions. Note that isolating a malicious node cannot trigger this case.

Evidence 4: Changing entry II. This evidence shows the proportion of changed entries in the case of different next hop (not the malicious node) and the same distance. We believe the impacts on the node communication should be very minimal in this case. Both attacks and countermeasures could cause this case.

Evidence 5: Changing entry III. This evidence points out the proportion of changing entries in the case of different next hop (not the malicious node) and the different distance. Similar to Evidence 4, both attacks and countermeasures could result in this evidence. The path change may also safest routing cost and transmission delay of the network. m(Insecure) = d, so m(Secure)=1-d On the other hand, 1-d is the maximum value of the belief that means the status of MANET is secure.

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 {¢, {Secure}, {Insecure}, {Secure, Insecure}}. Note that {Secure, Insecure} means the security state of MANET could be either secure or insecure, which describes the uncertainty of the security state. Bel{Insecure} is used to represent the risk of MANET.

Phase 2: Decision making phase

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 his goal.

Phase 3: Intrusion response phase

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.

Phase 4: Routing table recovery phase

In this approach, there are 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.

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.

Algorithm

The risk analyze response mechanism for MANET routing attacks are build upon following the Dempster-Shafer mathematical theory of evidence . It 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. In D-S theory, propositions are represented as subsets of a given set. Suppose θ is a finite set of states, and let 2 θ denote the set of all subsets of θ .D-S theory calls θ, a frame of discernment. 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 <m, IF> where m describes the basic probability assignment. Basic probability assignment function m is defined as follows:

m (θ)=0 and ∑m(A)=1.

The algorithm for combination of multiple evidences is constructed as follows

Algorithm 1: MUL-EDS-CMB

INPUT : Evidence pool Ep

OUTPUT: One evidence

1. |Ep| = size of(Ep);
2. While |Ep| > 1 do
3. Pick two evidences with the least IF in
4. Ep, named E1 and E2;
5. Combine these two evidences, E = <m1 ⍰
6. m2, (IF1 + IF2)/2 >;
7. Remove E1 and E2 from Ep;
8. Add E to Ep;

9. end

10. return the evidence in Ep.

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.

VI. CONCLUSION

In this paper 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, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

References

1. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
2. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.
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. 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.
5. G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.
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 ofIntrusion 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. M. Yamada and M. Kudo, "Combination of Weak Evidences byD-S Theory for Person Recognition," Knowledge-Based Intelligent Information and Engineering Systems, pp. 1065-1071, Springer, 2004.
12. 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.

