DOI: https://doi.org/10.53555/nncse.v2i3.457 Publication URL: http://nnpub.org/index.php/CSE/article/view/457

AN EFFICIENT RISK-AWARE, DISTRIBUTED CONTROL SYSTEM TO MINIMIZE ROUTING ATTACKS ON MANET

Swati M. Dahekar*[1], Yogesh Bhute[2]

*[1,2]*Department of Computer Science and Engineering, Abha Gaikwad-patil college of Engineering, Nagpur, India.*

[1]*swati.dahekar@gmail.com*, [2]*yog.bhute@gmail.com*

Corresponding Author: -

Email ID - swati.dahekar@gmail.com

Abstract: -

The topological nature of MANET (Mobile Ad-hoc Network) itself demands high security due to its mobility movement, but designing a risk aware routing path for MANET is a complex task because of its Dynamic nature of Infrastructure. In this proposal, designing a Dynamic routing path decider to find less risk aware routing path for effective communication.

The efficiency of the throughput and Routing failures can be further reduced by making Nodes of MANET to be more Knowledgeable that is with more Metadata parameters. This paper introduces a class of metrics to measure the effective security offered in a wireless network as a function of the routing topology and the link security provided by the key assignment protocol. This joint protocol analysis allows a network analyst or an adversary to evaluate the vulnerability of network traffic and isolate weakly secured connections. Its show how an intelligent adversary can mount a node capture attack using vulnerability evaluation to focus the attack on the nodes which contribute maximally to the compromise of network traffic.

Keywords: - *Mobile Ad-hoc Network, Risk aware, Multilevel-data, Routing attack, Distributed node, Attack detection, Attack Mitigation.*

I. INTRODUCTION

MOBILE Adhoc Networks (MANET) is 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 [1], [2] 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 abovementioned 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 [3]. 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. [4] 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 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 [5]. 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. DS 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], 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. 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. RELATED WORK

Ziming Zhao [Risk-Aware Response for Mitigating MANET Routing Attacks] 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. 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, propose a risk-aware response mechanism to systematically cope with the identified routing attacks. My risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factor. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of the packet delivery ratio and routing cost.

Y. Sun, W. Yu, Z. Han, and K. Liu, 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 trustworthiness of other nodes without centralized authorities. This paper presents an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. In the proposed framework, trust is a measure of uncertainty with its value represented by entropy. We develop four Axioms that address the basic understanding of trust and the rules for trust propagation. Based on these axioms, it presents two trust models: entropy-based model and probability-based model, which satisfy all the axioms. Techniques of trust establishment and trust update are presented to obtain trust values from observation. The proposed trust evaluation method and trust models are employed in ad hoc networks for secure ad hoc routing and malicious node detection. A distributed scheme is designed to acquire, maintain, and update trust records associated with the behaviors of nodes' forwarding packets and the behaviors of making recommendations about other nodes. Simulations show that the proposed trust evaluation system can significantly improve the network throughput as well as effectively detect malicious behaviors in ad hoc networks.

M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, Reputation management systems have been proposed as a cooperation enforcement solution in ad-hoc networks. Typically, the functions of reputation management (evaluation, detection, and reaction) are carried out homogeneously across time and space. However, the dynamic nature of ad-hocnetworks causes node behavior to vary both spatially and temporally due to changes in local andnetwork-wide conditions.

When reputation management functions do not adapt to such changes, their effectiveness, measured in terms of accuracy (correct identification of node behavior) and promptness (timely identification of node misbehavior), may be compromised it propose an adaptive reputation management system that realizes that changes in node behavior may be driven by changes in network conditions and that accommodates such changes by adapting its operating parameters. It introduced a time-slotted approach to allow the evaluation function to quickly and accurately capture changes in node behavior. It shows how the duration of an evaluation slot can adapt according to the network's activity to enhance the system accuracy and promptness. It then shows how the detection function can utilize a Sequential Probability Ratio Test (SPRT) to distinguish between cooperative and misbehaving neighbors. The SPRT adapts to changes in neighbors' behavior that are a by-product of changing network conditions, by using the node's own behavior as a benchmark. It compares the proposed solution to a non-adaptive system, showing the ability of the system to achieve high accuracy and promptness in dynamic environments. To the best of our knowledge, this is the first work to explore the adaptation of the reputation management functions to changes in network conditions.

P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A.Reninger ,This paper presents a new model for, or rather a new way of thinking about adaptive, risk-based access control. This paper basic premise is that there is always inherent uncertainty and risk in access control decisions that is best addressed in an explicit way. We illustrate this concept by showing how the rationale of the well-known, Bell-Lapadula model based; multi-level security (MLS) access control model could be used to develop a risk-adaptive access control model. This new model is more like a fuzzylogic control system than a traditional access control system and hence the name "fuzzy MLS". The long version of this paper is published as an IBM Research Report.

III. MOTIVATION

Existing System

Several works 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. 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. proposed a naïve 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.

Disadvantage of Existing System

However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning.

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 nonassociative 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.

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.

Dempster’s Rule

Associative. For DRC, the order of the information in the aggregated evidences does not impact the result. As shown in a non-associative combination rule is necessary for many cases.

Non-weighted. DRC implies that we trust all evidences equally. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence.

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

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

Dempster's Rule of Combination with Importance Factors

In this section, we propose a Dempster‟s rule of combination with importance factors. We prove our combination rule follows the properties defined in the previous section.

Theorem 1. Dempster's Rule of Combination with Importance Factors: Fig:

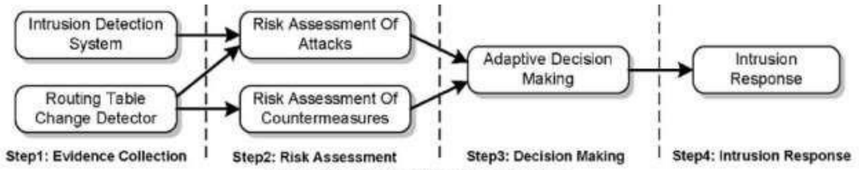
Intrusion Detection System
Routing Table Change Detector
Risk Assessment Of Attacks
Risk Assessment Of Countermeasures
Adaptive Decision Making
Intrusion Response
Step1: Evidence Collection
Step2: Risk Assessment
Step3: Decision Making
Step4: Intrusion Response

Fig: Risk-aware response mechanism.

Risk-aware response mechanism.

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 naive fuzzy-based method. In this section, we overview the OLSR and routing attacks on OLSR.

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 Adhoc 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. Routing Attack on OLSR 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 non existing paths to lure data packets.

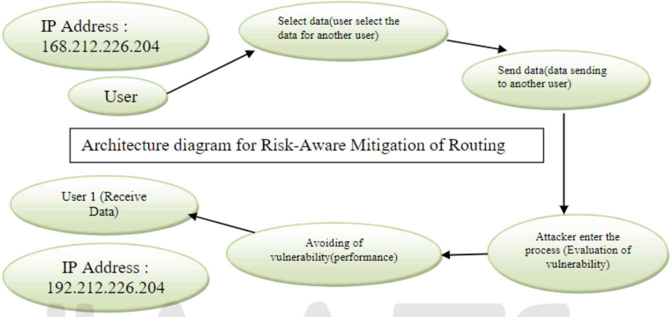
IP Address : 168.212.226.204
User
Select data(user select the data for another user)
Send data(data sending to another user)
Architecture diagram for Risk-Aware Mitigation of Routing
User 1 (Receive Data)
Avoiding of vulnerability(performance)
Attacker enter the process (Evaluation of vulnerability)
IP Address : 192.212.226.204

Fig: Architecture diagram for mitigation of Routing attacks

IV. CONCLUSIONS

In this paper malicious node in the MANET network is detected and isolated using DUMPSTERSHAFER mathematical theory. It broadcast alert message about the malicious node to all the nodes in the network so that all the nodes in the network will be aware of malicious node. And, hence it provides maximum security and trust worthiness in MANET routing.

REFERENCES

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

[2].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.

[3].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.

[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 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,” AIMagazine, vol. 5, no. 3, p. 81, 1984.