Risk Aware Mitigation for MANET Routing Algorithm

S. Balaji 1[#1], S. Thamizharasan 2[#2]

1 Final Year M. Tech (CSE), Christ college of Engineering and Technology, Puducherry-605010.
2 Final Year M. Tech (CSE), Christ college of Engineering and Technology, Puducherry-605010.

ABSTRACT

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 the first technique 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.

Keywords: Dempster-Shafer mathematical theory, mobile ad hoc network (MANET), Dempster's rule of combination with importance factors (DRCIF).

1. INTRODUCTION

In the recent year there are so many files and information are hacked by hackers while sending information through internet or intranet [1]. The main idea of this project is sending information from one system to another system in a secure manner using Dempster Shafer mathematical method in network security.

In this Paper 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 no 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 [2], considering damages caused by both attacks and countermeasures.

The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks [3]. We evaluate our response mechanism against representative attack scenarios and experiments. Our results clearly demonstrate the effectiveness and scalability of our risk-aware approach.

2. RELATED WORK

Several works addressed the intrusion response actions in MANET [4] 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] [6].

Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation.

3. PROPOSED CONCEPT

In this paper we propose an extended D-S evidence model [2] 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. 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.

4. PERFORMANCE ANALYSIS AND SIMULATIONS

Every project is feasible given unlimited resources and infinite time. Unfortunately, the development of a computer-based system is more likely to be plagued by resource scarcity and stringent delivery scheduled. It is both necessary and prudent to evaluate feasibility of a project at the earliest possible time.

Wastage of manpower of financial resources and untold professional embarrassment can be averted as if the ill conceived system is recognized in the definition phase. So, a detailed study was carried to check the work ability of the proposed system.

4.1 INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data into a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delays, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?

- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occurs.

4.2 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improve the system's relationship to help user decision-making.

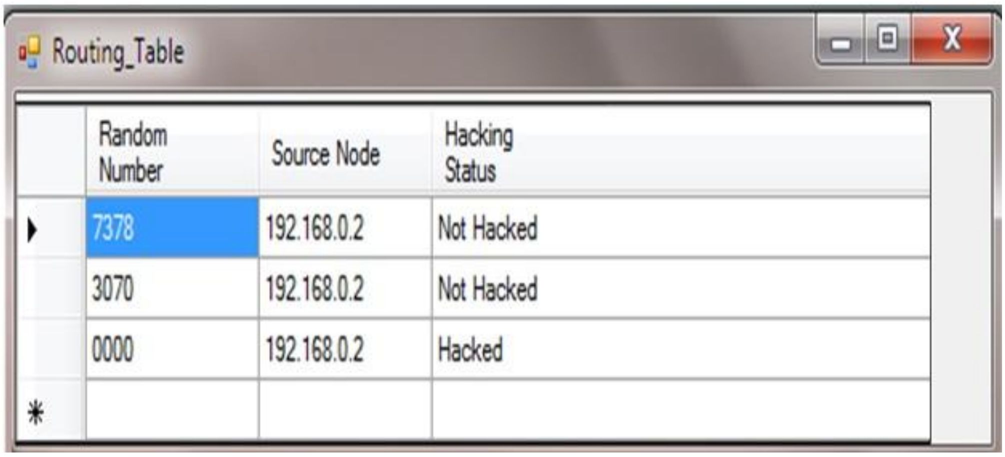
1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create documents, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.



	Random Number	Source Node	Hacking Status
▸	7378	192.168.0.2	Not Hacked
	3070	192.168.0.2	Not Hacked
	0000	192.168.0.2	Hacked
*			

Routing_Table Output Design

4.3 EXCEPTION HANDLING

In this the process of responding to the occurrence, during computation, of exceptions – anomalous or exceptional situations requiring special processing – often changing the normal flow of program execution. It is provided by specialized programming language constructs or computer hardware mechanisms.

In general, an exception is handled (resolved) by saving the current state of execution in a predefined place and switching the execution of a specific subroutine known as an exception handler. If exceptions are continual, the handler may later resume the execution at the original location using the saved information. For example, a floating point divide by zero exception will typically, by default, allow the program to be resumed, while an out of memory condition might not be resolvable transparently.

4.4 SECURITY

A network based concept is used for security purpose. While sending information on system to another system we need computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of networking.

5. CONCLUSION

In this paper, we have presented 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 a more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

REFERENCE

[1] 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.

[2] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET,” IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.

[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. 127145, 2007.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, “ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks,” ACM Trans. Information and System Security, vol. 10, no. 4, pp. 1-35, 2008.

[6] 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.

[7] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, “A Specification-Based Intrusion Detection Model for OLSR,” Proc. Ninth Int’l Symp. Recent Advances in Intrusion Detection (RAID ’06), pp. 330-350, 2006.

[8] C. Tseng, S. Wang, C. Ko, and K. Levitt, “DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for Manet,” Proc. Ninth Int’l Symp. Recent Advances in Intrusion Detection (RAID ’06), pp. 249-271, 2006.