AWARE MITIGATION FOR MANET ROUTING ATTACKS

[1]Bendalam Vijay, [2]Jallu Swathi

Sr. Assistant Professor, Assistant Professor
Department of CSE, Department of ECE
AITAM, Tekkali, Srikakulam, Andhra Pradesh, India

***ABSTRACT*: MOBILE Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has 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.**

Due to infrastructure less Manets are easily deployable to malicious nodes. Hence extended Dempster theory was used for the evidence collection to minimize the attacks hence the mathematical calculations was done to collect the evidence there by collecting the evidence the source will identify the malicious nodes and no data will send to that nodes thereby it protect the data and this type of security mechanism was employed in the manets.

INTRODUCTION

1.1MOTIVATION

The motivation of our application is to reduce the risk in MANET routing attacks. There are 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. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

1.2 PROBLEM DEFINITION

Consider one scenario i.e., while we are sending some information from SOURCE to DESTINATION in ADHOC environment, 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.

LITERATURE SURVEY

2.1 INTRODUCTION

MOBILE Ad hoc Networks (MANET) 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.

Due to infrastructure less Manets are easily deployable to malicious nodes. Hence extended Dempster theory was used for the evidence collection to minimize the attacks hence the mathematical calculations was done to collect the evidence there by collecting the evidence the source will identify the malicious nodes and no data will send to that nodes thereby it protect the data and this type of security mechanism was employed in the manets.

2.2 EXISTING SYSTEM

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. 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 MANET. Their cost model took subjective knowledge and objective MANET. Their cost model took subjective knowledge and objective evidence into account omitted as seamless combination of two properties with logical reasoning

2.3 DISADVANTAGES OF EXISTING SYSTEM

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

2.4 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 DS 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.

2.4.1 MODULES

Evidence collection

In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing data Change Detector (RDCD) runs to figure out how many changes on routing data are caused.

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 her 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.

2.5 ADVANTAGES OF PROPOSED SYSTEM

- Manets have high beneficiary to the users because it didn't have any access point, so the devices which are used in transmission are acts as routers and access point for the data transfer.

- It is easily established network ,cost will be less, data transfer is very easy and in high security

ANALYSIS

3.1 INTRODUCTION

The analysis is the process of understanding the system at a greater depth, identifying the missing functions with an intention to improve it through better method and procedures. The requirement analysis is done in order to understand the problem, the Software system is to solve. Requirements analysis is on identifying what is needed from the system, not how the system will achieve its goals. The goal of requirements specification phase is to produce the software requirements specifications document. The person responsible for the requirements analysis is often called the analyst.

In this phase we study the system and observe the problem of existing system and think how to cover the problems (problem analysis). There are three major activities in this phase are problem analysis, feasibility study and software requirement specification. The requirement document must specify all the functional and performance requirements, the formats of inputs and outputs and all design constraints that exist due to political, economic, environment and security reasons.

The phase ends with validation of the requirements specified in the document.

Validation is often done through "requirement review", in which a group of people including representatives of the client critically reviews the requirement specifications.

3.2 Feasibility Study

All projects are feasible if they have unlimited resources and infinite time. But the development of software is plagued by the scarcity of resources and difficult delivery rates. It is necessary and prudent to evaluate the feasibility of a project at the earliest possible time. The three considerations are involved in the feasibility analysis.

Economic feasibility

This procedure is to determine the benefits and savings that are expected from a candidate system and compare with cost. If benefits outweigh cost then the decision is made to design and implement the system. Otherwise further justification or alterations in proposed system that have to be made if it is having a change of being approved .This is an ongoing effort that improves in accuracy of each phase of the system lifecycle. For my project I am not expecting any feasibility costs spent on this on this project because here I am using open source environments.

Technical feasibility

Technical feasibility centers on the existing mobile system (hardware, software etc...) and to what extent it can support the proposed addition if the budget is a serious constraint, then the project is judged not feasible. The Technical feasibilities are important role in my project because here I am using android operating system.

Operational feasibility

People are inherently resistant to change and mobiles have been known to facilitate change. In my project a technical people require to configure the software and technical background is necessary to work on the sensors.

7.3 VALIDATION

Validation aims to demonstrate that the software functions in a manner that can be reasonably expected by the customer. This test is the conformance of the software to the Software Requirements Specification.

CONCLUSION

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.

FUTURE EXPANSION

Future scope of this project is as it is a simulation we can use this in the adhoc networking so that we can reduce the attacks which happen repeatedly in these infrastructure less environment.

REFERENCES

Books Referred

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

[2] R. Yager, "On the Dempster-Shafer Framework and New Combination

Rules_1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

[3] 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.

[4] 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.

[5] S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l

[6] Symp. Recent Advances in Intrusion Detection (RAID '07), pp. 127- 145, 2007.

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

Website Browsed

[1] http://java.sun.com

[2] http://www.sourcefordgde.com

[3] http://www.networkcomputing.com/

[4] http://www.roseindia.com/

[5] http://www.java2s.com/