INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Identifying Misbehaving Nodes Using Evidence Calculation IDs In MANETs

P.Elakkiya
Department of CSE, Srinivasan engineering college, Perambalur, India

C.Subramanian
Department of CSE, Srinivasan engineering college, Perambalur, India

Abstract:

A Mobile Ad Hoc Network (MANET) is a dynamic wireless network, in which each node communicate with each other without the use of pre-existing infrastructure or centralized administration. Many other applications like law enforcement, public meeting, virtual class room and some military applications has been using MANETs. It has been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Here Routing Attacks have caused the most devastating damage to Manet. Earlier system typically attempt to isolate malicious nodes based on naive and binary fuzzy response decisions which may results in the unexpected network partition and could lead to uncertainty in countering routing attacks. In this paper, we propose risk-aware response mechanism with evidence calculation intrusion detection system to systematically cope with the identified routing attacks in Manet, which is based on the extended Dempster-Shafer Mathematical Theory of Evidence and articulate expected properties for Dempster's rule of combination with important factors (DRCIF), to measure the risk of attacks and countermeasures.

Key words: *Mobile ad hoc Networks, Intrusion retort, Risk responsive, Dempster-Shafer Theo*

1.Introduction

A Manet is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. With the increase of cheaper, smaller, and more powerful mobile devices, mobile ad hoc networks have become one of the fastest growing area of research. This new type of self-organizing system combines wireless communication with a high degree node mobility.

Unlike conventional wired networks, they have no fixed infrastructure. The union of nodes forms an subjective topology. This flexibility makes them attractive for many applications such as military applications, where the network topology may change rapidly to reflect a force's equipped movements, and disaster recovery operations, where the fixed infrastructure may be non-operational and many other applications like emergency reprieve scenarios, law enforcement, open meeting, virtual class room. The Ad hoc self-organisation is suitable for virtual conferences, where setting up a fixed network infrastructure is a time consuming high-cost task

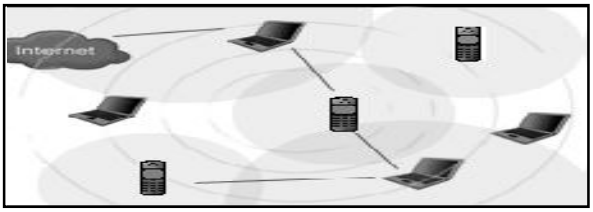

Figure 1

In MANET scenario, improper countermeasures may cause the unexpected network separation, bringing supplementary damages to the network infrastructure. To address the above-mentioned decisive issues, more flexible and adaptive response should be investigated.

Risk assessment is still a nontrivial, demanding problem due to its involvements of individual knowledge, intention evidence, and logical reasoning. One of the main challenges in Manet is to design the robust security solution that can protect Manet from various routing attacks. Many Routing Protocols has been proposed, but do not consider security.

Existing Routing protocols counter selfish activities by forcing the selfish nodes to cooperate. Existing key management mechanisms are usually based on central points where services such as certification authorities or key servers can be placed. Since Manet do not have such points, new key management mechanisms have had to be developed to fulfill requirements. Existing solutions typically attempt to isolate malicious nodes based

on binary or naive fuzzy response decisions. Nevertheless, binary responses may result in the unexpected network detachment, causing additional damages to the network infrastructure, and naive fuzzy response could escort to ambiguity in countering routing attacks. In Proposed System to protect Manet, Risk Aware Response Mechanism systematically cope with the identified routing attacks through the use of Optimized Link State routing protocol based on extended Dempster Shafer Theory Of Evidence which focus on important factors and articulate expected properties for Dempster's rule of combination with important factors (DRCIF).

2.Related Work

During the past decade, a number of techniques have been proposed to predict the intruder and to protect manets from various routing attacks. Cheng.P propose a method based on Fuzzy Multi Level Security, a new access control model, which in a limited context can be used to quantify risk associated with information access. Chang et al. propose a method based on On-demand routing protocol are more appropriate for wireless environments because they initiate a route discovery process only when data packets need to be routed. Jia and Gong propose AODV relies on dynamically establishing route table entries at intermediate nodes. Li et al. propose trust value which is a level of likelihood with which an agent will perform a particular action before such action can be monitored and in a context in which it affects our own actions. Recently, several algorithms have been proposed to avoid intruder in manet coverage area. Hennings–Yeomans et al. propose Authorization Enforcement Facility analyzes incoming traffic and determines the amount of risk associated with each source. Zou and Yuen discover Reputation management systems can target security concerns related to internal misbehavior attacks in decentralized and unstructured networks. Hu.Y propose a method on On-demand routing protocol are more appropriate for wireless environments because they initiate a route discovery process only when data packets need to be routed.

Some ad hoc network routing protocols require shared private keys between all pairs of nodes in the network. Private-key distribution is substantially more challenging public-key distribution because protocols for key distribution must ensure the secrecy of such keys.

In many ad hoc networks, the compromise of a single network node and the capture of its cryptographic keys is a possible threat. are based on the fundamental constraints that the

super-resolution image should generate the low resolution input images when appropriately warped and down-sampled to model the image formation process.

Dempster-Shafer Theory (DST) is a mathematical theory of evidence. In a finite discrete space, Dempster-Shafer theory can be interpreted as a generalization of probability theory where probabilities are assigned to sets as opposed to mutually select singletons. In fixed probability theory, evidence is associated with only one possible event. In DST, evidence can be connected with multiple possible events, e.g., sets of events. As a effect, evidence in DST can be meaningful at a higher level of notion without having to resort to assumptions about the events within the evidential set where the evidence is sufficient enough to permit the mission of probabilities to single events, the Dempster-Shafer model collapse to the fixed probabilistic formulation.

3.Problem Definition And Architecture

Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Along with these attacks, routing attacks have received extensive attention since it could cause the most devastating damage to MANET

Earlier there is binary fuzzy and naïve response decisions is considered. binary responses may result in the unpredicted network division causing supplementary damages to the network infrastructure, and nai¨ve fuzzy responses could lead to ambiguity in countering routing attacks in MANET.To overcome this we moves to the proposed system.

The architecture diagram of the project is given below which describe the flow of the process. Here before a packet could be transmitted have to find shortest path and predict the intruder and should transmit the packet in a secure way.

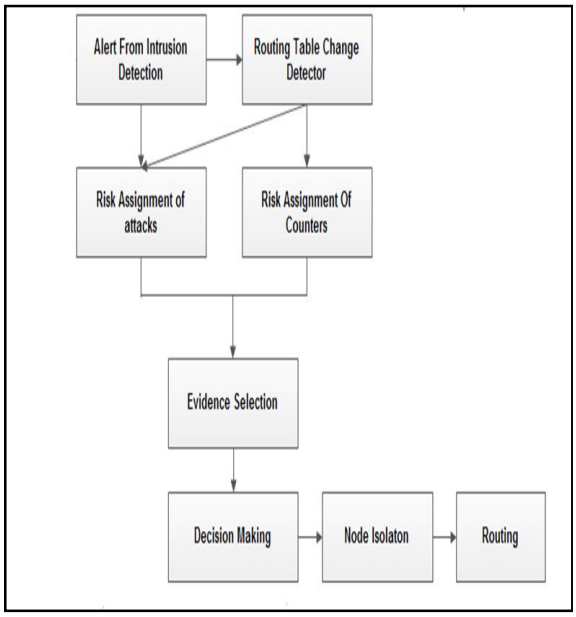

Figure 2

4.Algorithms

4.1.Evidence Calculation Intrusion Detection

Risk-Aware Response system is distributed, which means each node in the system makes its own response decisions based on the evidences and its own individual benefits. Hence, some nodes in Manet may isolate the malicious node, but others may still keep in support with due to high dependency relationships. Risk Aware Response mechanism is divided into 5 steps:

Evidence Collection: 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 Assignment: 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 Dempster-Shafer Theory. Risk of countermeasures is calculated as well during a risk assessment time. Based on the threat of attacks and the risk of countermeasures, the entire risk of an attack could be figure out.

Decision Making For Risk: The adaptive decision module provides a flexible retort decision-making mechanism, which takes risk inference and risk acceptance into

account. To alter temporary remoteness level, a user can set different thresholds to fulfill the goal.

Response for Intrusion: With the output from risk evaluation and decision-making module, the consequential response actions, including routing table recovery and node isolation, are carried out to alleviate attack damages in a distributed manner.The following describes the activities associated with each stage:

Before attack- Arbitrary packets were generated and transmitted among nodes without activating any of them as attackers.

After attack- Specific nodes were set as attackers which conducted malicious activities for their own income. Though, any detection or response is not available in this stage.

After response- Response decisions for each node were made and conceded out based on three different mechanisms.

Node Isolation: To perform a node isolation response, the neighbours of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting any packets from it. On the other hand, a binary node separation reply may result in negative impacts to the routing operations, even bringing more routing damage than the attack itself.

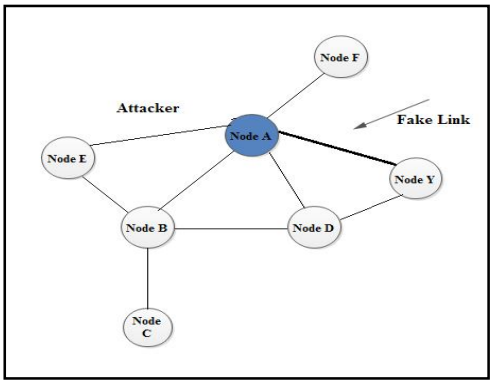

Figure 3

5.Optimized Link State Routing Protocol (OLSR)

Optimized Link State Protocol (OLSR) is a proactive routing protocol, so the routes are always instantaneously available when needed.

OLSR is an optimization version of a pure link state protocol. So the topological changes cause the flooding of topological in sequence to all available hosts in the network. To reduce the possible transparency in the network protocol uses Multipoint Relays (MPR). The idea of MPR is to reduce flooding of broadcasts by reducing the same broadcast in

some regions in the network. One more reduce is to provide the shortest path. The falling time interval for the control messages transmission can bring more reactivity to the topological changes.

OLSR uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for result the information about the link status and the host's neighbours. With the Hello message the Multipoint Relay (MPR**)** Selector set is construct which describe the neighbours has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs. The Hello messages are sent only one hop away but the Topology Control messages are transmit throughout the complete network. TC messages are used for propagating information about own advertise neighbours which includes at least the MPR Selector list. The TC messages are broadcasted occasionally and only the MPR hosts can forward the TC messages.

6.Extended Dempster shafer Theory Of Evidence

Notion of importance factors:

- Importance factor (IF) is a positive real number allied with the importance of evidence. IFs are derivative from chronological observations or expert experiences.
- An evidence E is a 2-tuple $\langle m, IF \rangle$ where m describes the basic probability assignment. Basic Probability assignmet functions are as follows:

$$m(\varphi) = 0 \qquad (1)$$

$$\sum_{A \subseteq \Theta} m(A) = 1 \qquad (2)$$

$$Bel(A) = \sum_{B \subseteq A} m(B) \qquad (3)$$

Dempster's Rule Of Combination with Important factors:

- No belief have to be committed to φ in the result of our combination rule.
- The total belief have to be equal to 1 in the result of our combination rule.
- If the importance factors of each evidence are identical, our Dempster's rule of grouping should be equal to Dempster's rule of grouping without importance factors.

- Importance factors of each evidence must not be transferable

7.Conclusion

This paper has been studied to get a clear view of the problem to be addressed. In the proposed system extended Dempster-Shafer theory of evidence with a notion of importance factors have been used in order to measure the risk of both attacks and countermeasures. Moreover, Optimized Link State Routing protocol provides an optimized path when compared to Link state Routing Protocol. It is seen that using Evidence Calculation Intrusion Detection system can be more advantageous than using binary or naive fuzzy response.

Secure Packet Forwarding are the focus of our future work.

8.Acknowledgment

I take this chance to express my deep sense of gratitude to our Management, our principal Dr. B. Karthikeyan , for providing an excellent infrastructure and support to pursue this research work at our college. I express my profound thanks to Head of the department Prof. J. Mercy Geraldine M.E.,(Ph.D) for her administration and keen interest, which motivated me along the course as well as research work, and also thank to all staff members.

9.Reference

1. Cheng.P, Rohatgi.P, Keser.C, Karger.P, Wagner.G, and Reninger.A, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy, 2007.
2. Deng.H, Li.W, and Agrawal.D, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
3. Hu.Y and Perrig.A, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.
4. Hu.Y, Perrig.A, and Johnson.D, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, no. 1, pp. 21-38, 2005.
5. Perkins.C, Belding-Royer.D, and Das.S, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
6. Refaei.M, DaSilva.L, Eltoweissy.M, and Nadeem.T, "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. Sun.Y, Yu.W, Han.Z, and Liu.K, "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.
8. Teo.T, Ahn.G, and Zheng.Y, "Dynamic and Risk-Aware Network Access Management," Proc. Eighth ACM Symp. Access Control Models and Technologies (SACMAT '03), pp. 217-230, 2003.
9. Wu.H, Siegel.M, Stiefelhagen.R, and Yang.J, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.