A Novel Framework for Mitigating Routing Attacks in Manet

Chinna Reddy Varalakshmi [*], R.Kumaran [**]

[*] M.Tech Student SVCET, R.V.S.Nagar, Chittor.,
** Assistant Professor, Dept. of CSE, SVCET, R.V.S.Nagar, Chittor.

Abstract- ***A set of Mobile nodes which are self configuring and connected by set of wireless links through a set of per defined automatic routing protocol. In Mobile Ad hoc Networks there different types of high vulnerable attacks due to dynamic and very large area of infrastructure. In various MANET attacks routing attacks are very high risk aware activities which are to be given a high attention. In Existing MANET risk aware mechanism is not able to cope with routing attacks. The IDS used in the existing system is having a very limited response mechanism, we require a enhanced new frame work for more efficient detection routing attacks in MANET. The routing attacks makes the network to use same ID with multiple nodes in the network, Information Exchange, Domain and Space Detection of routing attacks in the network are increased. To reduce the network damage an advanced risk ware mitigating routing protocols to be designed. In intrusion detection system we have many techniques to mitigate various critical attacks but, existing solutions are only attempt to isolate malicious nodes using fuzzy or binary decisions. But this decisions may in unexpected networks are causing more additional damages to the network infrastructure in MANET. The project is designed to propose a new risk aware response mechanism in a systematic way with identified routing attacks. Our approach is an extension DS theory of mathematics for introducing various factors of notion. The designed approach provides more effectiveness in controlling attacks in MANET with a increased performance..***

Manuscript: Chinna Reddy Varalakshmi, *M.Tech, SVCET, R.V.S.Nagar, Chittor.*
Email: lucky.chinnareddy@gmail.com
R.Kumaran *B.Tech.,M.E., Assistant Professor, Dept of Computer Science Engineering, SVCET, R.V.S.Nagar, Chittor*

I. INTRODUCTION

A MANET network is a infrastructure less and network of mobile devices availability of the wireless media to interconnect various mobile devices in exchange of information between mobile nodes. The open media of these networks leaves it at a risk to multiple routing and security threats for wireless packet transmissions. Users with a transceiver can snoop on wireless packet transmissions, inject spurious messages, or attack legitimate ones. While routing attack activities for dropping and message infusion with an injection can be prevented using advanced IDS methods, Various Internal and External attacks are much difficult and harder and difficult to control because of open area packet transmission and initially MANET are open networks processing various types of Medias and signals processed? They have been shown to actualize and control various severe routing attacks against various MANET networks. In the easiest form of routing attacks, the proposed interferes are to be controlled with the reception of Acknowledgement messages by transmitting a unremitting routing signal between various intermediate nodes, or several short node pulses. In General routing attacks have been considered to be an Internal and external threat model to the routing activities of MANET, in which the mobile nodes are not part of the network. Under this model we can control

continuous random transmission of higher power interference signals of various routing strategies. The advanced adopting a DS algorithm has several disadvantages and cannot control all the attacks. In the First Section, the adversary has to disburse a significant amount of energy to control signal frequency band width of interest. In the Second section, the uninterrupted presence of extraordinarily high interfering levels makes this type of attacks easy to detect. Several various methods are addressed to control the intrusion response actions in MANET by the behaviors of intrusions using a isolating uncooperative nodes. The malicious nodes are neglected to most possible negative side effects with intrusion attacks. The network infrastructure may be damaged in unexpected networks with the existing method, to overcome and address the damages for critical issue a adaptive response is investigated in this research.

The proposed research provides effective support with adaptive techniques to control the routing attacks in MANET. The challenging problems which are involved of subjective knowledge and objective evidence with logical reasoning, where getting the previous experience is called Subjective knowledge, and getting the previous result outputs are objective evidence and formal foundation is called logical reasoning. The proposed paper uses DS (Dempster Shafer) mathematical theory provides a solution in a traditional probability algorithm for showing representing uncertainty. The theory of D-S evaluates and secures information with valuable tool. In the research the first section represents subjective and objective activities of evidences with prospect assignment. In the second section DS rule of combination (DRC) to combine several evidences together with probable reasoning. Various DS Rule combines solution a solution to several limitations of existing techniques. To overcome the limitations of MANET intrusions we proposed DS rule combination with importance factors model in DS. The proposed project provides a enhanced risk aware response mechanism in a systematic procedure to control routing attacks in MANET. The proposed methods controls routing attacks and save time with a isolation method. The proposed DS method is linked to Optimized Link State Routing Protocol is simulated with the experiment with a passive MANET routing protocol.

II. RELATED WORK

In existing systems, D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by various other engineering fields, where precise measurement is impossible to obtain or expert elicitation is required. D-S theory support Dempster‟s rule of combination (DRC) to combine several evidences together with probable reasoning. However, as identified in, Dempster‟s rule of combination has limitations, such as treating equally without differentiating every evidence and considering priorities among them. To solve this limitations in MANET intrusion response scenario, a new Dempster‟s rule of combination with a notion of importance factors (IF) in D-S evidence model was introduced. Here a risk-aware response mechanism was proposed to systematically cope with routing attacks in MANET, but now adaptive time-wise isolation meth- od is proposed. The risk-aware approach is based on the extended D-S evidence model. Then to simulate the proposed concept they used a proactive MANET routing protocol called Optimized Link State Routing protocol (OLSR)

Based on the behavior of attackers, these attacks can be classified into passive or active attacks. Again it is categorized as outsider and ins ider attacks. In routing packet attacks, attackers could not only prevent existing paths from being used, but also spoof nonexistent paths

to lure data packets to them.

III. EXISTING AND PROPOSED SYSTEM

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 while logical reasoning requires a formal foundation. Wang et al. proposed a naı¨ve 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.

Disadvantages

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

•During communication, replica is forced to generate challenge key along with their movements by which replica attack is easily detected by the proposed scheme.

•No limitation on number of replicas in a network.

•Use of 1-way hash function results, low computation overhead.

•It provides high detection accuracy.

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 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, 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.

Advantages

•Our approach takes advantage of this capability by assuming that we have a large number of mobile relay nodes.

•In the other hand, due to low manufacturing cost, existing mobile sensor platforms are typically powered by batteries and only capable of limited mobility.

•Consistent with this constraint, our approach only requires one-shot relocation to designated positions after deployment. Compared with our approach, existing mobility approaches typically assume a small number of powerful mobile nodes, which does not exploit the availability of many low-cost mobile nodes

IV. MODULES DESCRIPTION

Evidence collection

In this step, 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 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.

Routing table recovery

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.

V.CONCLUSION

MANET is distinguished from other networks mainly by its self configuring and optimizing nature. Being the flexible network, MANET is exposed to various kinds of attacks especially the routing attacks. There are various methods introduced to mitigate such critical attacks such as intrusion detection techniques. The proposed mechanism called risk aware response solution designed in the research has provided a potential control for various damages. The System provides various security rules and monitors the routing activities to find Intruders with irregularities of performance and gives alarm alert to the system administrator for the future actions. Though sever techniques have proposed earlier were not given better performance from network damages. To control the critical issues and provide a flexible and adaptive mechanism this investigation of risk aware mechanism improved the efficiency of controlling the attacks and improved the security with faster bandwidth. To propose the risk aware mechanism we have used DS theorem. 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.

VI. FUTURE WORK

In our future enhancement we have planned to extend our investigation with trajectory clustering mechanism. The idea of clustering can be provided concurrent checking of intruders in routing transmissions. The clustering mechanism minimizes the objective of functioning activities proposed in the current work. The enhancement provides a seeded rounded clustering for the route to provide more enhanced security with low values in network descriptor.

REFERENCES

[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] 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.

[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," AI Magazine, vol. 5, no. 3, p. 81, 1984.

[10] R. Yager, "On the Dempster-Shafer Framework and New Combination Rules1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

[11] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.

[12] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.