*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 4 (Jul. - Aug. 2013), PP 75-78*
*www.iosrjournals.org*

# Risk Assessment for Identifying Intrusion in Manet

M. Siva Shankar Reddy[1], D. Raman[2]
[1]*M.Tech in Computer Science and Engineering,Vardhaman College of Engineering, Hyderabad, India.*
[2]*Associate Professor , Department of Computer Science and Engineering,Vardhaman College of Engineering, Hyderabad, India.*

***Abstract:*** *In this paper we have taken one of the most amazing network concepts which makes network simpler. By considering the aspect of both side as of good and its related issues like most important and unavoidable is i.e. "Security". Hence, enhancing the security in wireless networks has become of vital importance. In this perspective of concept, we mainly study two security aspects of wireless networks. One is service confidentiality and access control that is to ensure only legitimate users can access service data according to their privileges and in other perspective is of service attack. Wireless broadcast is a convenient and effective approach for disseminating data to a number of users. User training in computer and network security is crucial to the survival of modern networks, yet the methods employed to train users often seem ineffective. The secrecy issues in the context of mandatory and discretionary access control in a multilevel networked environment. Hence of, we stressed on two aspects key management scheme is proposed to address secrecy and efficiency in broadcast services, where keys are used for service confidentiality and access control.*
***Keywords:*** *Security, Unauthorized Access, Authentication*

**Submitted date 21 June 2013** **Accepted Date: 26 June 2013**

## I. Introduction

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. 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.

In computer networking, a packet drop attack or blackhole attack is a type of denial of service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

The packet drop attack can be frequently deployed to attack wireless ad-hoc network. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

## II. Headings

At the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**Modules:**

- **Evidence collection**
- **Risk assessment**
- **Decision making**
- **Intrusion response**
- **Routing table recovery**

**1 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.

**2 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.

**3 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.

**4 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.

**5 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

## III. Figures And Tables

Wireless network trend become the most viable part of the network in these days, which needs some of the issues to be rectified. In recent years, many researchers have studied the limitations of the security mechanisms that protect wireless networks. If we consider the statistical data of wireless devices which shows the sales of embedded wireless devices grows 66.2% each year [12]. Fig.1.1 shows that hot spots are becoming more frequent in public areas such as airports, hotels, and retail stores. Newer generations of mobile computing equipment come with wireless support standard. In 2003, 55% of laptops sold had embedded wireless support built in [12], and this percentage is expected to grow even more due to technologies like Intel's Centrino chip. Indeed, from corporate networks to home networks, the number of wireless networks and clients is on the rise. Wi-Fi has undertaken a remarkable journey in the space of just a few short years. It is a journey that has been defined by a global spread of investment by network operators, the integration of Wi-Fi as a key component of a heterogeneous network strategy, the emergence of new and innovative business models and, perhaps most importantly, by a strengthening of user dependence on Wi-Fi. It is now widely accepted that operators wishing to provide a complete set of broadband-based services to their customers will need to do.

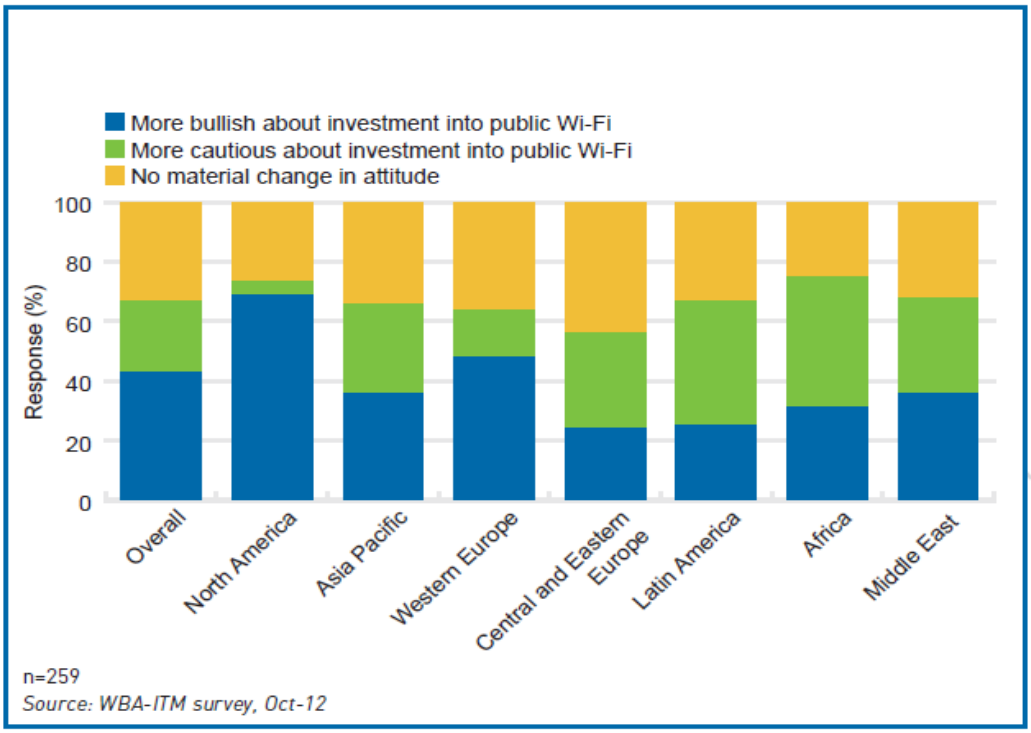


Fig1.1: Attitude of company towards Wi-Fi

## IV. 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 riskaware 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. problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular, we are concerned with a simple yet effective attack in which a router selectively drops packets destined for some Victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Previous detection protocols have tried to address this problem with a user-defined threshold: too many dropped packets imply malicious intent. However, this heuristic is fundamentally unsound; setting this threshold is, at best, an art and will certainly create unnecessary false positives or mask highly focused attacks. We have designed, developed, and implemented a compromised router detection protocol that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions.

## 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,feb 2006, 305-317

[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, may 2010,707-719

[3]. 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), 2008pp. 35-48

[4]. K. Sentz and S. Ferson, "Combination of Evidence in Dempster- Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002

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

[6]. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.

[7]. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, May/june 2004, 28- 39

[8]. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), 2008pp. 1-10.
[9]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09),2009 pp. 355-370.
[10]. J. R. Boston, "ASignal Detection System Based on Dempster-ShaferTheory and Comparison to Fuzzy Detection", IEEE Transactions onSystems, Man, and Cybernetics, Part C:Applications and Reviews, Volume30, Issue 1, February 2000.
[11]. 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), 2006, 330-350.
[12]. J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, march/april2011, 233-245.
[13]. S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Int'l J. Network Security, vol. 105, no. 627,2006 ,65-68.
[14]. T. Toth and C. Kruegel, "Evaluating the Impact of Automated Intrusion Response Mechanisms," Proc. 18th Ann. Computer Security Applications Conf. (ACSAC '02), 2002, 9-13.
[15]. C. Strasburg, N. Stakhanova, S. Basu, and J. Wong, "Intrusion Response Cost Assessment Methodology," Proc. Fourth ACM Symp. Information, Computer, and Comm. Security (ASIACCS '09),2009, 388-391.
[16]. L. Teo, G. Ahn, and Y. Zheng, "Dynamic and Risk-Aware Network Access Management," Proc. Eighth ACM Symp. AccessControl Models and Technologies (SACMAT '03),2003, 217-230.