International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

RISK-AWARE RESPONSE ANSWER FOR MITIGATING PAINTER ROUTING ATTACKS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

Risk-Aware Response Answer For Mitigating Painter Routing Attacks

Mounika Reddy Avula[1], Deepak Ekkati[2], Kalyani Dharavath[3], Kranthi Gande[4], Shoban Babu Sriramoju[5]

[1]*Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India*

[2]*Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India*

[3]*Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India*

[4]*Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India*

[5]Associate Professor, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

Abstract – Mobile Adhoc Networks (MANET) is extremely liable to attacks attributable to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received extensive attention since it may cause the foremost devastating injury to painter if there exists many intrusion response techniques to mitigate such crucial attacks, existing solutions usually arrange to isolate malicious nodes supported binary or naive fuzzy response selections. However, binary responses could lead to the sudden network partition, inflicting extra damages to the network infrastructure, and naive fuzzy responses may lead to uncertainty in countering routing attacks in painter. During this paper, we tend to propose a risk-aware response mechanism to consistently deal with the known routing attacks. Our risk-aware approach relies on an extended Dempster-Shafer mathematical theory of proof introducing a notion of importance factors. Additionally, our experiments demonstrate the effectiveness of our approach with the thought of many performance metrics.

Keywords: Mobile unintended networks, intrusion response, risk aware, dempster-shafer theory.

----------♦----------

INTRODUCTION

MOBILE Adhoc Networks (MANET) are utilized to line up wireless communication in makeshift environments while not a predefined infrastructure or centralized administration. Therefore, painter has been commonly deployed in adverse and hostile environments wherever central authority purpose isn't necessary. Another distinctive characteristic of painter is that the dynamic nature of its configuration which might be oft modified attributable to the unpredictable quality of nodes. what is more, every mobile node in painter plays a router role whereas transmission knowledge over the network. Hence, any compromised nodes beneath an adversary's management may cause vital injury to the practicality and security of its network since the impact would propagate in performing arts routing tasks may work [1], [2] self-addressed the intrusion response actions in painter by uninflected uncooperative nodes supported the node name derived from their behaviors. Such a straightforward response against malicious nodes usually neglects attainable negative aspect effects committed the response actions. In painter situation, improper countermeasures could cause the sudden network partition, transferal extra damages to the network infrastructure. To handle the higher than mentioned crucial problems, additional versatile and reconciling response ought to be investigated. The notion of risk is adopted to support additional reconciling responses to routing attacks in painter [3]. However, risk assessment remains a nontrivial, difficult downside attributable to its involvements of subjective data, objective proof, and logical reasoning. Subjective data may be retrieved from previous expertise and objective proof may be obtained from observation whereas logical reasoning needs a proper foundation. Wang et al. [4] projected a naive

fuzzy cost-sensitive intrusion response answer for painter. Their value model took subjective data and objective proof under consideration however omitted a seamless combination of 2 properties with logical reasoning. During this paper, we tend to get how to bridge this gap by exploitation Dempster-Shafer mathematical theory of proof (D-S theory), that offers another to ancient applied mathematics for representing uncertainty [5]. D-S theory has been adopted as a valuable tool for evaluating reliableness and security in data systems and by alternative engineering fields [6], [7], wherever precise measure is not possible to get or knowledgeable stimulation is needed. D-S theory has many characteristics. First, it allows North American country to represent each subjective and objective evidence with basic chance assignment and belief performs. Second, it supports Dempster's rule of combination (DRC) to mix many evidences at the side of probable reasoning. However, as known in [8], [9], [10], [11], Dempster's rule of combination has many limitations, like treating proofs equally while not differentiating every evidence and considering priorities among them. To handle these limitations in painter intrusion response situation, we tend to introduce a replacement Dempster's rule of combination with a notion of importance factors (IF) in D-S proof model.

II. REALATEDWORK

Some analysis efforts are created to hunt preventive solutions [21], [22], [23], [24] for shielding the routing protocols in painter. Though these approaches will forestall unauthorized nodes from connection the network, they introduce a big overhead for key exchange and verification with the restricted intrusion elimination. Besides, prevention-based techniques are less useful to deal with malicious insiders World Health Organization possesses the legitimate credentials to speak within the network. So, here we tend to propose a risk-aware response mechanism to consistently deal with routing attacks in painter, proposing an reconciling time-wise isolation methodology. Our risk-aware approach relies on the extended D-S proof model. So as to judge our mechanism, we tend to perform a series of simulated experiments with a proactive painter routing protocol, Optimized Link State Routing Protocol (OLSR) [12].

The foremost contributions of this paper are summarized as follows:

- We formally propose AN extended D-S proof 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, that has not been addressed within the literature.

- We propose a reconciling risk-aware response mechanism with the extended D-S proof model, considering damages caused by each attacks and countermeasures. The addictiveness of our mechanism permits North American country to consistently deal with painter routing attacks.

- We judge our response mechanism against representative attack eventualities and experiments. Our results clearly demonstrate the effectiveness and measurability of our risk-aware approach.

III. IMPLEMENTATION

OLSR Protocol

The major task of the routing protocol is to find the topology to make sure that every node will acquire a recent map of the network to construct routes to its destinations. Many economical routing protocols are projected for painter. These protocols typically represent one in all 2 major categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, like unintended On Demand Distance Vector (AODV) protocol [13], nodes notice routes only if they have to send knowledge to the destination node whose route is unknown. In distinction, in proactive routing protocols, like OLSR, nodes acquire routes by periodic exchange of topology data with alternative nodes and maintain route data all the time. OLSR protocol could be a variation of the pure Link-state Routing (LSR) protocol and is intended specifically for painter. OLSR protocol achieves optimization over LSR through the employment of multipoint relay (MPR) to produce AN economical flooding mechanism by reducing the amount of transmissions needed. Unlike LSR, wherever each node declares its links and forward messages for his or her neighbors, solely nodes elect as MPR nodes ar liable for advertising, likewise as forwarding AN MPR selector list publicized by alternative MPRs

IV. EXTENDED DEMPSTER-SHAFER THEORY FOR PROOF

The Dempster-Shafer mathematical theory of proof is each a theory of proof and a theory of probable reasoning. The degree of belief models the proof, whereas Dempster's rule of combination is that the procedure to combination and summarizes a corpus of evidences. However, previous analysis efforts determine many limitations of the Dempster's rule of combination

1. Associative: For DRC, the order of the data within the collective evidences doesn't impact the result. As shown in [10], a non-associative combination rule is critical for several cases.

2. No weighted: DRC implies that we tend to trust all evidences equally [11]. However, in reality, our trust to take issue completely different evidences. In alternative words, it means that we

should always take into account numerous factors for every proof. However Dempster-Shafer theory with importance factors will overcome each of the same limitations

Importance Factors and Belief perform

In D-S theory, propositions are portrayed as subsets of a given set. Suppose X could be a finite set of states, and let a pair of X denote the set of all subsets of X. D-S theory calls X, a frame of discernment. Once a proposition corresponds to a set of a frame of discernment, it implies that a specific frame discerns the proposition. First, we tend to introduce a notion of importance factors. Importance issue (IF) could be a positive complex quantity related to the importance of proof. IFs are derived from historical observations or knowledgeable experiences.

Defining a pair of a proof E could be a 2-tuple (m, IF), wherever m describes the essential chance assignment [5]. Basic chance assignment performs m is outlined as follows:

Add (m (A)) =1/A is sub set of X

According to [5], a perform Bel : 2X---[0,1] could be a belief perform over x if it's given by below equation for a few basic

Probability assignment m: 2X --- [0,1]

Bel (A) = sum (m (B)) /B is set of A

RISK-AWARE RESPONSE MECHANISM

Because of the infrastructure-less design of painter, our risk-aware response system is distributed, which suggests every node during this system makes its own response selections supported the evidences and its own individual edges. Therefore, some nodes in painter could isolate the malicious node, however others should still confine cooperation with attributable to high dependency relationships. Our risk aware response mechanism is split into the subsequent four steps shown in Fig.1. proof assortment. during this step, Intrusion Detection System (IDS) offers AN attack alert with a confidence price, and so Routing Table modification Detector (RTCD) runs to work out what number changes on routing table ar caused by the attack.
Risk assessment Alert confidence from IDS and also the routing table dynamic data would be more thought-about as freelance evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated likewise throughout a risk assessment section. Supported the chance of attacks and also the risk of countermeasures, the complete risk of AN attack may be discovered.
Decision creating. The reconciling call module provides a versatile response decision-making mechanism, that takes risk estimation and risk tolerance under consideration. To regulate temporary isolation level, a user will set completely different thresholds to satisfy her goal Intrusion response. With the output from risk assessment and decision-making module, the corresponding response actions, together with routing table recovery and node isolation, are distributed to mitigate attack damages during a distributed manner.

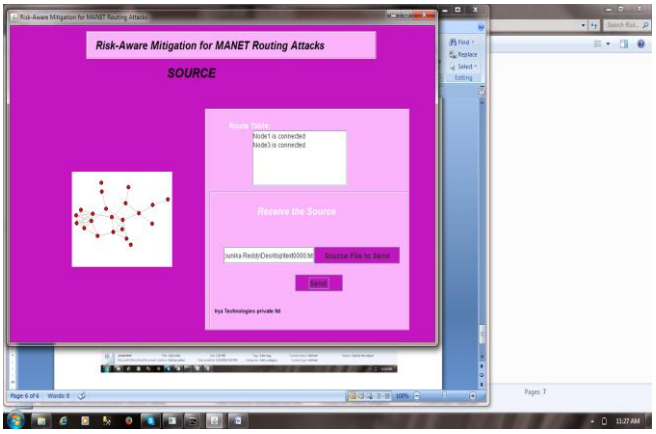

Fig-1 : Risk-aware response mechanism

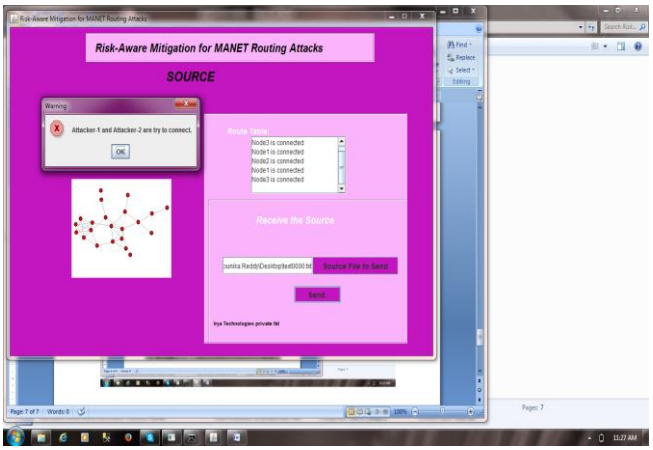

Fig 2 : Example situation

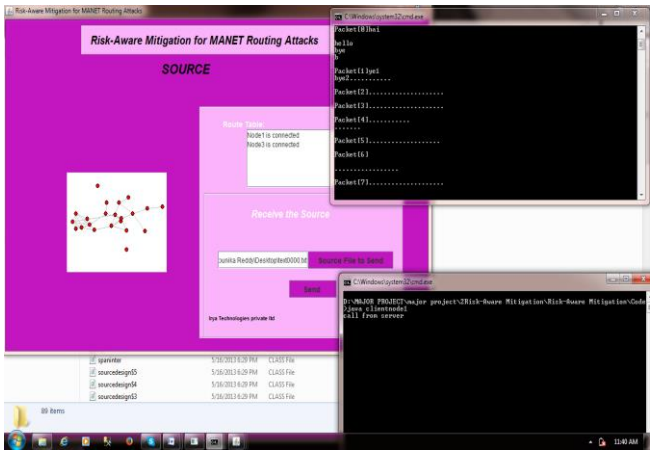

Fig 3: Packet Overhead

V. CONCLUSION

We have projected a risk-aware response answer for mitigating painter routing attacks. Especially, our approach thought-about the potential damages of attacks and counter measures. so as to live the chance of each attacks and counter measures, we tend to extend Dempster-Shafer theory of proof with a notion of importance factors supported many metrics, we tend to additionally investigated the performance and utility of our approach and also the experiment results clearly incontestable the effectiveness and measurability of our risk aware approach supported the promising results obtained through these experiments, we'd more get additional systematic thanks to accommodate node name and attack frequency in our reconciling call model

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