Handling Of Manet Routing Attacks Using Risk Aware Mitigation Based On D-S Theory

Ms. A. Dhivya, Dr. N. Saravanaselvam, Mrs. G. Rajeswari

Abstract— **In MANET (Mobile Ad hoc Networks) is highly vulnerable to attacks in this Routing attacks are most important because they will cause devastating damage to MANET. In order to deal with the routing attacks in the existing system we are using the binary or naive-fuzzy theory of cost sensitive intrusion response system in MANET. But this model cause unexpected network partition and additional damage, It took the subjective knowledge and objective evidence but omitted the logical reasoning part. So in proposed system we are using the risk aware response mechanism based on the quantitative risk estimation and tolerance.**

Key words: ***Mobile ad hoc networks, intrusion response, risk aware, dempster-shafer theory***

I. INTRODUCTION

MOBILE Adhoc Networks (MANET) area unit used to line up wireless communication in jury-rigged environments while not a predefined infrastructure or centralized administration. Therefore, Edouard Manet has been ordinarily deployed in adverse and hostile environments where central authority purpose is not necessary Another distinctive characteristic of Edouard Manet is that the dynamic nature of its topology which might be often modified thanks to the unpredictable quality of nodes. what is more, every mobile node in Edouard Manet plays a router role whereas transmission information over the network. Hence, associatey compromised nodes underneath an adversary's management might cause vital injury to the practicality and security of its network since the impact would propagate in performing arts routing tasks.

In Edouard Manet state of affairs, improper countermeasures may cause the sharp network partition, delivery any damages to the network infrastructure. to manage the preceding crucial issues, plenty of versatile and accommodative response have to be compelled to be investigated. Risk assessment remains a nontrivial, tough draw back as a results of its involvements of subjective info, objective proof, and logical reasoning. Subjective info could be retrieved from previous experience and objective proof could be obtained from observation whereas logical reasoning desires a correct foundation.

Wang et al. [2] projected a naive fuzzy cost-sensitive intrusion response declare Edouard Manet. Their worth model took subjective info and objective proof into account but omitted a seamless combination of two properties with logical reasoning. throughout this paper, we've a bent to induce how to bridge this gap by exploitation Dempster-Shafer mathematical theory of proof (D-S theory), that gives another to ancient math for representing uncertainty [3]. D-S theory has been adopted as a valuable tool for evaluating responsibility and security in information systems and by different engineering fields [4] where precise activity isn't doable to induce or knowledgeable stimulant is required. D-S theory has several characteristics. First, it permits u. s. of America to represent every subjective and objective evidences with basic likelihood assignment and belief perform. Second, it supports Dempster's rule of combination (DRC) to combine several evidences beside probable reasoning. However, as well-known in [5], [6], Dempster's rule of combination has several limitations, like treating proofs equally whereas not differentiating each proof and considering priorities among them. to manage these limitations in Edouard Manet intrusion response state of affairs, we've a bent to introduce a replacement Dempster's rule of combination with a notion of importance factors (IF) in D-S proof model.

II. ROUTING ATTACK

Based on the behavior of attackers, attacks against MANET can be classified into passive or active attacks. Attacks is any classified as either outsider or corporate executive attacks. With relevance the target, attacks might be additionally divided into knowledge packet or routing packet attacks. In routing packet attacks, attackers couldn't solely forestall existing methods from getting used, however additionally spoof non existing methods to lure knowledge packets to them. Several studies have been carried out on modeling MANET routing attacks. Typical routing attacks include black hole, fabrication, and modification of various fields in routing packets (route request message, route reply message, route error message, etc.). All these attacks could lead to serious network dysfunctions.

In terms of attack vectors, a malicious node will disrupt the routing mechanism within the following easy ways: 1st, it changes the contents of a discovered route, modifies a route reply message, associate

degreed causes the packet to be born as an invalid packet; then, it validates the route cache in different nodes by advertising incorrect methods, and refuses to participate within the route discovery process; and eventually, it modifies the contents of a knowledge packet or the route via that the information packet is meant to travel or behave ordinarily throughout the route discovery method however is born.

In OLSR, any node will either modify the protocol messages before forwarding them, or produce false messages or spoof associate degree identity. Therefore, the wrongdoer will abuse the properties of the choice formula to be elect as MPR. The worst case is that the potential choice of the attacker as the only MPR of a node. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation.

III. EXTENDED DEMPSTER SHAFER THEORY

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 mixture and summarize a corpus of evidences. However, previous analysis efforts establish many limitations of the Dempster's rule of combination.

1. ***Associative.*** *For DRC, the order of the information in the aggregated evidences does not impact the result. As shown in [6], a nonassociative combination rule is necessary for many cases.*

2. ***Nonweighted.*** *DRC implies that we trust all evidences equally. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence.*

A. Importance factors and belief function

In D-S theory, propositions are represented as subsets of a given set. Suppose Θ is a finite set of states, and let 2^{Θ} denote the set of all subsets of Θ. D-S theory calls Θ a frame of discernment. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors.

1. Definition: Importance factor (IF) is a positive real number associated with the importance of evidence. IFs are derived from historical observations or expert experiences.

2. Definition: An evidence E is a 2-tuple (m, IF), where m describes the basic probability assignment [3]. Basic probability assignment function m is defined as follows:

$$m(\Phi)= 0 \quad (1)$$

$$\sum_{A \in \Theta} m(A)=1 \quad (2)$$

According to [5], a function Bel : 2^{Θ} ->[0,1] is a belief function over Θ if it is given by (3) for some basi probability assignment m: 2^{Θ} -> [0,1];

$$Bel(A)= \sum_{B \in A} m(B) \quad (3)$$

for all $A \in 2^{\Theta,}$ Bel(A) describes a measure of the total beliefs committed to the evidence A.

Suppose Bel1 and Bel2 are belief functions over the same frame Θ, with basic probability assignments m1 and m2. Then, the function m : 2^{Θ} -> [0,1];defined by m(Φ)= 0 and

$$m(C) = \frac{\sum A_i \cap B_j = C \; m1(A_i)\, m2(B_j)}{1-\sum A_i \cap B_j = \Theta \; m1(A_i)\, m2(B_j)} \quad (4)$$

3. Definition: Extended D-S evidence model with importance factors: Suppose E1=‹m1,IF1› and E2 =‹m2, IF2› are two independent evidences. Then, the combination of E1 and E2 is E= ‹m1⊕m2, (IF1 +IF2)/2›, where ⊕ is Dempster's rule of combination with importance factors.

B. Properties of dempster's rule of combination with importance factors

The projected rule of combination with importance factors have to be compelled to be a superset of Dempster's rule of combination. throughout this section, we've an inclination to explain four properties that a candidate Dempster's rule of combination with importance issue have to be compelled to follow. Properties one and one or two of certify that the combined result's a legitimate proof. Property 3 guarantees that the primary Dempster's Rule of Combination may be a special case of Dempster's Rule of Combination with importance factors, where

the combined evidences have constant priority. Property four ensures that importance factors of the evidences square measure freelance from each other.

Property 1. No belief ought to be committed to _ in the result of
our combination rule

$$m'(\Phi)= 0 \quad (5)$$

Property 2. The total belief ought to be equal to 1 in the result of our combination rule

$$\sum_{A \in \Theta} m'(A)=1 \quad (6)$$

Property 3. If the importance factors of each evidence are equal, our Dempster's rule of combination should be equal to Dempster's rule of combination without importance factors

$$m'(A,IF1,IF2)= m(A) \text{ ,if } IF1=IF2 \quad (7)$$

for all A € Θ, where m(A) is the original Dempster's Combination Rule.

Property 4. Importance factors of each evidence must not be exchangeable

$$m'(A,IF1,IF2) \neq m'(A,IF1,IF2) \text{ if } (IF1 \neq IF2) \quad (8)$$

C. *Dempster's rule of combination with importance factors*

Proposed DRCIF is non associative for multiple evidences. Therefore, for the case within which ordered data isn't obtainable for a few instances, it's necessary to form the results of combination in line with multiple evidences. Our combination algorithmic rule supports this demand and therefore the complexness of our algorithmic rule is O(n), wherever n is that the variety of evidences. It indicates that extended Dempster-Shafer theory demands no further procedure value compared to a naı¨ve fuzzy-based methodology. The algorithmic rule for combination of multiple evidences is built as follows:

Algorithm 1. MUL-EDS-CMB

INPUT: Evidence pool Ep
OUTPUT: One evidence

1 | Ep | = sizeof(Ep);
2 While | Ep | > 1 do
3 Pick two evidences with the least IF in Ep,
named E1 and E2;
4 Combine these two evidences,
E= ‹ m1 ⊕ m2,(IF1 , IF2)/2›;
5 Remove E1 and E2 from Ep;
6 Add E to Ep;
7 end
8 return the evidence in Ep

IV. RISK AWARE RESPONSE MECHANISM

In this section, we have a tendency to articulate an adjustive risk-aware response mechanism supported quantitative risk estimation and risk tolerance. rather than applying easy binary isolation of malicious nodes, our approach adopts an isolation mechanism in a very temporal manner supported the danger price. we have a tendency to tend to perform risk assessment with the extended D-S proof theory introduced in Section for every attacks and corresponding countermeasures to make extra correct response picks illustrated in Fig. 1.

A. *General Idea*

Because of the infrastructure-less design of Manet, our risk-aware response system is distributed, which suggests each node throughout this method makes its own response choices supported the evidences and its own individual edges. Therefore, some nodes in Manet could isolate the malicious node, however others should still detain cooperation with as a result of high dependency relationships. Our risk aware response mechanism is divided into the following four steps shown in Fig. 1.

1. **Evidence collection**. In this step Intrusion Detection System (IDS) provides associate degree attack alert with a confidence price, and so Routing Table modification Detector (RTCD) runs to work out what percentage changes on routing table area unit caused by the attack.

2. **Risk evaluation.** Alert confidence from IDS and therefore the routing table would be additional thought-about as freelance evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated moreover throughout a risk assessment section. supported the danger of attacks and thus the chance of countermeasures, the whole risk of associate attack is also discovered.

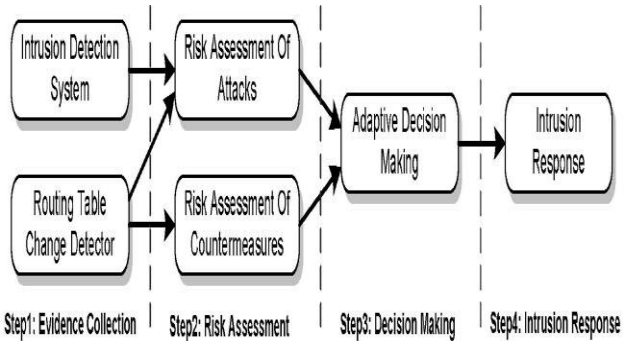

Fig 1. Risk-aware response mechanism.

3. **Decision creating.** The accommodative decision module provides a flexible response decision-making mechanism, that takes risk estimation and risk tolerance into consideration. to control temporary isolation level, a user can set fully totally different thresholds to satisfy her goal.

4. **Intrusion response.** With the output from risk assessment and decision-making module, the corresponding response actions, at the side of routing table recovery and node isolation, ar administered to mitigate attack damages throughout a distributed manner.

B. Reaction of routing attacks

In the approach, use two different responses to deal with different attack methods: routing table recovery and node isolation. Routing table recovery includes native routing table recovery and world routing recovery. native routing recovery is performed by victim nodes that observe the attack and automatically recover its own routing table. World routing recovery involves with inflicting recovered routing messages by victim nodes and alter their routing table supported corrected routing knowledge in real time by different nodes in painter. Node isolation may even be the foremost intuitive due to forestall any attacks from being launched by malicious nodes in painter. To perform a node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packets through it nor settle for any packets from it.

C. Risk evaluation

Since the attack response actions may cause more damages than attacks, the risks of both attack and response should be estimated. We classify the security states of MANET into two categories: {Secure, Insecure}. In other words, the frame of discernment would be {Φ,{Secure},{Insecure}, {Secure, Insecure}} Note that {Secure, Insecure} means the security state of MANET could be either secure or insecure, which describes the uncertainty of the security state. Bel{Insecure} is used to represent the risk of MANET.

a. Selection of evidance

Evidence choice approach considers subjective proof from experts' information and objective proof from routing table modification. we have a tendency to propose a unified analysis approach for evaluating the risks of each attack ($Risk_A$) and step ($Risk_C$). Take the arrogance level of alerts from IDS because the subjective information conspicuous one. In terms of objective proof, analyze whole completely different routing table modification cases. There area unit staple items in OLSR routing table (destination, next hop, distance). Thus, routing attack can cause existing routing table entries to be unintelligible, or any item of a routing table entry to be changed. We illustrate the possible cases of routing table change and analyze the degrees of damage in Evidences 2 through 5.

Evidence 1: Alert confidence. the boldness of attack detection by the IDS is provided to deal with the likelihood of the attack incidence.

Evidence 2: Missing entry. This proof indicates the proportion of missing entries in routing table. Link withholding attack or node isolation step will cause potential deletion of entries from routing table of the node.

Evidence 3: ever-changing entry I. This proof represents the proportion of fixing entries within the case of next hop being the malicious node.

Evidence 4: ever-changing entry II. This proof shows the proportion of modified entries within the case of various next hop (not the malicious node) and therefore the same distance.

Evidence 5: ever-changing entry III. This proof points out the proportion of fixing entries within the case completely different|of various} next hop (not the malicious node) and therefore the different distance. like proof four, each attacks and countermeasures might end in this proof.

b. Combination of evidance

Call the combined evidence for an attack, EA and the combined evidence for a countermeasure, EC. Thus, Bel_A(Insecure) and Bel_C(Insecure) represent risks of attack ($Risk_A$) and countermeasure ($Risk_C$), respectively. The combined evidences, E_A and E_C are defined and the entire risk value derived from $Risk_A$ and $Risk_C$

$$E_A = E_1 \oplus E_2 \oplus E_3 \oplus E_4 \oplus E_5,$$

$$EC = E2 \oplus E4 \oplus E5,$$

where $\oplus$ is Dempster's rule of combination with important factors defined in Theorem 1

$Risk = Risk_A - Risk_C = Bel_A(Insecure) - Bel_C(Insecure)$.

D. Adaptive decision making

The response level is as well divided into multiple bands. each band is said to academic degree isolation degree, that presents a special amount of your time of the isolation action. The response action and band boundaries unit all determined in accordance with risk tolerance and may be changed once risk tolerance threshold changes. the upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would keep each node intact. The band between the upper tolerance threshold and lower tolerance threshold is said to the temporary isolation response, inside that the isolation time (T) changes dynamically supported the assorted response level given by following equation where n is that the vary of bands which i is that the corresponding isolation band.

V. RESULT

The performance ends up in these random network topologies of our risk-aware approach with DRCIF, risk-aware approach with DRC and binary isolation approach. In Fig. 2, because the range of nodes will increase, the packet delivery magnitude relation conjointly will increase as a result of there square measure a lot of route decisions for the packet transmission. Among these 3 response mechanisms, we have a tendency to conjointly notice the packets delivery magnitude relation of our DRCIF risk-aware response is on top of those of the opposite 2 approaches.

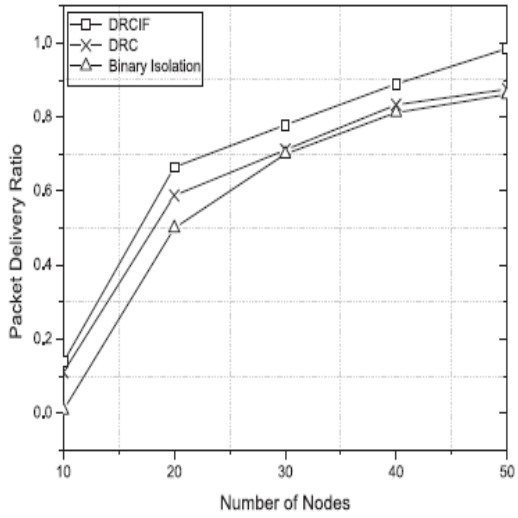

Fig. 2 Packet delivery ratio

In Fig. 3, we are able to observe that the routing price of our DRCIF risk-aware response is under those of the opposite 2 approaches. Note that the fluctuations of routing price shown in Fig. three are caused by the random traffic generation and random placement of nodes in our realistic simulation. In our DRCIF risk-aware response, the amount of nodes that isolate the malicious node is a smaller amount than the opposite 2 response mechanisms.

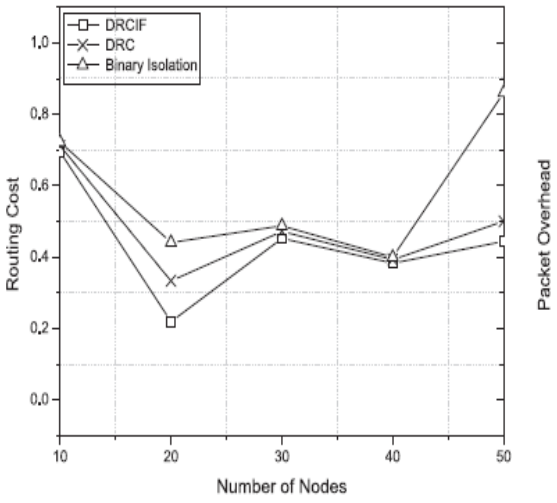

Fig 3. Routing cost

In Fig 4 , that's the reason why we can also notice that as the number of nodes increases, the packet overhead and the using our DRCIF risk-aware response

are slightly higher than those of the other two response mechanisms.

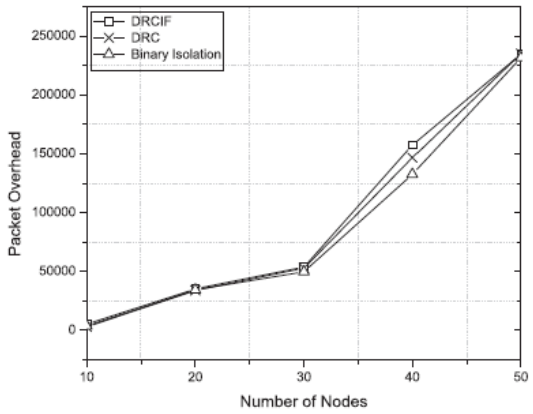

Fig. 4 Packet Overhead

In Fig. 5the mean latency victimization our DRCIF risk-aware response is over those of the opposite 2 response mechanisms, once the amount of nodes is smaller than twenty. However, once the amount of nodes is bigger than twenty, the mean latency victimization our approach is a smaller amount than those of the opposite 2 response mechanisms.

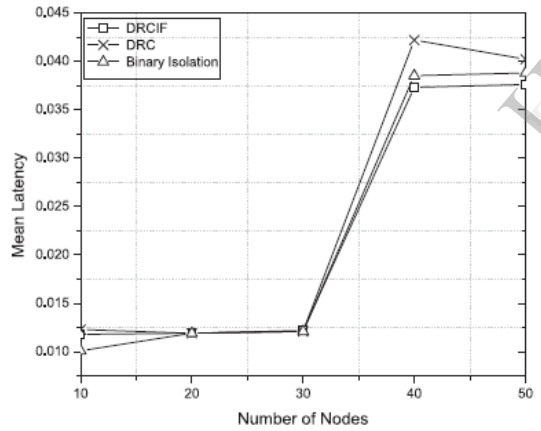

Fig.5 Mean Latency

VI. CONCLUSION

Risk-aware response answer for mitigating Manet routing attacks. Especially, our approach considered the potential damages of attacks and countermeasures. so as to live the danger of each attacks and countermeasures, we tend to extended 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 quantifiable of our risk aware approach. supported the promising results obtained through these experiments

REFERENCES

[1] [1] Ziming Zhao, Gail-Joon Ahn ,"Risk-Aware Mitigation for MANET Routing Attacks " IEEE transactions on dependable and secure computing, vol. 9, no. 2, March/April 2012

[2] 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.

[3] 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.

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

[5] 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.

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

[7] R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

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

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

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85- 91, Oct. 2007.

[11] L.Teo, G. Ahn, and Y. Zheng, "Dynamic and Risk Aware Network Access Management," Proc. Eighth ACM Symp. Access Control Models and Technologies (SACMAT '03), pp.217-230,2003.

AUTHORS PROFILE

Ms. A. Dhivya received his B.E degree in the area of Computer Science And Engineering from Anna University, Chennai, Tamilnadu, India in 2007. Doing M.E in the area of Computer Science And Engineering in Sree Sowdambika College of Engineering, Aruppukottai

Dr.N.Saravanaselvam M.E, PhD / Dean Academic in Sree Sowdambika College Of Engineering, Aruppukottai

Mrs.G.Rajeswari M.E / AP in Sree Sowdambika College Of Engineering, Aruppukottai