Intrusion Response with Dempster Shafer theory of evidence to detect and overcome routing attack in Mobile Ad hoc Networks

Mr. S. G. Phule[1], Mr. G. T. Chavan[2]

[1] *Student, Computer Engineering Department, Sinhgad College of Engineering Savitribai Phule Pune University, Maharashtra, India*
[2] *Associate. Prof., Computer Engineering Department, Sinhgad College of Engineering Savitribai Phule Pune University, Maharashtra, India*

---***---

Abstract - *Mobile Ad hoc Networks are extremely exposed to attacks because of the self-motivated nature of its network infrastructure. Out of all these attacks, routing attacks need sizeable attention since it could root the most upsetting harm to MANET. There exist several intrusion response techniques to mitigate such critical attacks, still the existing solutions typically attempt to isolate malicious node based on immature unclear response decisions. However these responses may consequence in the unforeseen network separation, causing supplementary damages to the network infrastructure, and also could lead to ambiguity in countering routing attacks in MANET. In this paper an intrusion response mechanism is proposed to thoroughly deal with the recognized routing attacks. This approach is based on an extended Dempster-Shafer mathematical theory of evidence with belief of value factors. Also result shows the helpfulness of this approach.*

Key Words: Mobile Ad hoc Networks, Intrusion Response, Dempster-Shafer theory

1. INTRODUCTION

Mobile Ad hoc Network is a self governing system of movable nodes connected by wireless links. Every node functions as a router to move on packets in addition to act as an end system. The nodes are free to move about and systemize themselves into network. These nodes change location repeatedly. A number of attacks are likely in MANET and among them routing attack could cause the worst damage. Quite a few work [1], [2], [3] concentrate on the intrusion response actions in MANET by separating un-cooperative nodes based on the node reputation derived from their behaviors. These responses often neglects the potential harmful side effects caught up with the response actions. These improper countermeasures in MANET may cause unexpected network separation. In this paper, Dempster Shafer Theory is used which has several characteristics. First one is, it facilitate us to describe both subjective and objective evidences with basic probability assignment & belief function. Second it supports Dempster rule of combination to combine several evidences together with probable reasoning. To tackle the limitations of this Dempster rule of combination Dempster rule of combination with value factors in DS evidence model is introduced. In this paper a response mechanism to thoroughly cope with routing attacks in MANET is proposed. The paper structuring is as follows: Section II provides the related work in MANET intrusion detection & response systems. Section III provides problem definition Section IV express how our extended D-S Evidence model can be incorporated with value factors & mathematical modeling. Section V conveys fine points of our intrusion response mechanism. Section VI shows the result snapshots. Section VII concludes the paper

2. RELATED WORK

A number of study efforts have been made to look for preventive solutions [11], [12], [13], [14] for protecting the routing protocols in MANET. Even though these approaches can prevent illegal nodes from joining the network, they bring in a major operating cost for key exchange and verification with the limited intrusion removal. Besides, prevention based techniques are less supportive to deal with malicious insiders who hold the genuine identification to communicate in the network. Many IDSs for MANET have been lately introduced. Due to the nature of MANET, most IDS are structured to be distributed and have a supportive architecture. Similar to signature-based and anomaly-based IDS models for the wired network, IDSs for MANET use specification-based or statistics-based approaches. Specification-based approaches, like [15], observe network behavior and evaluate them with identified attack features, which are impractical to deal with new attacks. On the other hand, statistics-based approaches, such as Watchdog [16], and [17], evaluate network behavior with typical behavior patterns, which consequence in higher false positives rate than specification-based ones. Because of the existence of false positives in both MANET IDS models, intrusion alerts from these systems always go together with alert confidence, which indicates the likelihood of attack incident. Intrusion response system (IRS)[18] for MANET is encouraged by MANET IDS. In [9] and [10], malicious nodes are cut off based on their reputations. Their effort fails to take benefit of IDS alerts and straightforward separation may root surprising network partition. Wang et al.[19] brought the idea of cost-sensitive intrusion response which considers topology dependency and attack damage. The benefit of the solution presented here is to put together evidences from IDS, local routing table with expert information, and countermeasures with a mathematical reasoning approach.

Risk-aware approaches. When it comes to make response decisions [20], there always exist natural ambiguity which leads to unpredictable risk, particularly in security and intelligence arena. Risk-aware approaches are introduced to deal with this difficulty by complementary action benefits and harm trade-offs in a quantified way. [21] applied dynamic risk-aware mechanism to decide whether an access to the network should be denied or allowed.

3. PROBLEM DEFINITION

In MANET, improper countermeasures in MANET may cause unexpected network separation However, risk judgment is still a nontrivial challenging difficulty due to its involvements of subjective knowledge, objective evidence, and logical reasoning. [19] projected a immature unclear cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a flawless mixture of two properties with logical reasoning. [22] adopted Dempster-Shafer theory to calculate the risk of attacks and responses. However, as acknowledged in [23], their model with Dempster's rule treats evidences uniformly without differentiating them from each other. The majority of the effort addressed the intrusion response actions in MANET by separating uncooperative nodes based on the node reputation resulting from their behaviors. Such a straightforward response against malicious nodes often neglects probable negative side effects caught up with the response actions. In MANET set-up, inappropriate countermeasures may cause the surprising network partition, bringing added damages to the network infrastructure. To deal with this drawback, this paper presents a Dempster's rule of combination with a concept of value factors in DS evidence model.

4. EXTENDED DEMPSTER-SHAFER THEORY OF EVIDENCE

The Dempster-Shafer Mathematical theory of evidences is both a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dempster rule of combination is the procedure to aggregate and summarize a corpus of evidences. However previous research efforts identify several limitations of the Dempster's rule of combination [4].

Associative For DRC, the order of the information in the aggregated evidences doesn't impact the result.

Non Weighted DRC implies that we trust all evidences equally [6]. However in reality our trust on different evidences may differ. In another words it means we should consider various factors for each evidence. [8] Proposed rules to combine several evidences for first limitation. However, the weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security & criticality.

Value Factors and Belief Functions

In DS 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. DS theory calls Θ a frame of discernment. When a proposition corresponds to a subset of frame of discernment, it implies that a particular frame discerns the proposition.

Definition 1. Value Factor (VF) is a positive real number linked with the significance of evidence.

Definition 2. An Evidence E is a 2-tuple <m,VF>, where m describes the basic probability assignment [5]. Basic probability assignment function m is defined as follows:

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

and

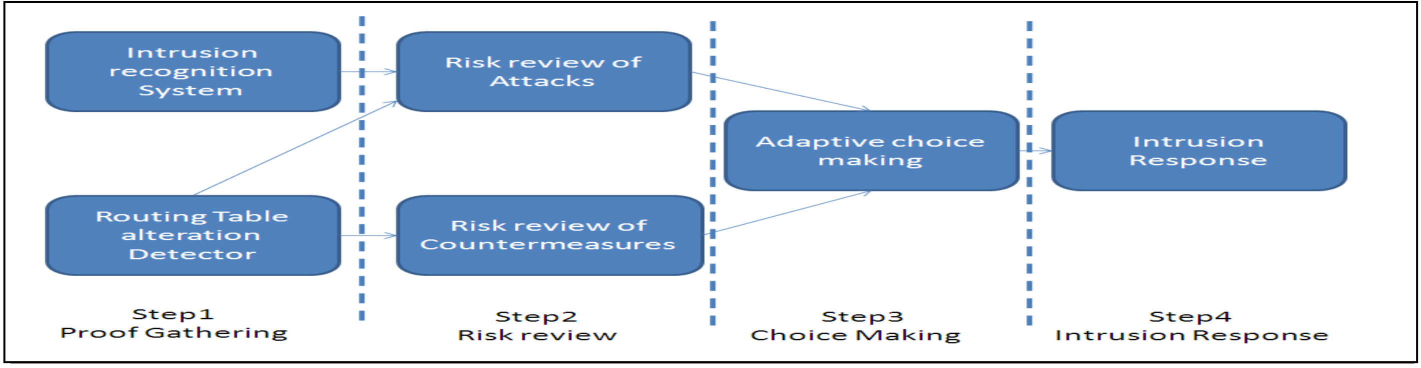
$$\sum_{A\subseteq\Theta} m(A) = 1 \qquad (2)$$

According to [4], a function bel:2^{θ} →[0,1] is a belief function over θ if it is given by (3) for some basic probability assignment m: 2^{θ} →[0,1]

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

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

Given several belief functions over the same frame of discernment and based on distinct bodies of evidence, Dempster rule of combination, which is given by (4),



enables us to compute the orthogonal sum, which describes the combined evidence.
Suppose Bel_1 & Bel_2 are belief functions over the same frame θ, with basic probability assignment m_1 and m_2. Then the function m: $2^\theta \rightarrow [0,1]$ defined by $m(\Phi) = 0$ and

$$m(C) = \frac{\sum_{A_i \cap B_j = C} m_1(A_i) m_2(B_j)}{1 - \sum_{A_i \cap B_j = \phi} m_1(A_i) m_2(B_j)} \qquad (4)$$

for all non empty $C \subseteq \Theta$, m(C) is a basic probability assignment which describes the combined evidence.
Suppose VF_1 and VF_2 are Value factors of two independent evidences named E_1 and E_2, respectively. The combination of these two evidences implies that our total belief to these two evidences is 1, but in the same time, our belief to either of these two evidences is less than 1. And we define the Value factors of the combination result equals to $(VF_1+VF_2)/2$.
Definition 3. Extended D-S Evidence model with Value factors: Suppose $E_1 = <m_1, VF_1>$ and $E_2=<m_2,VF_2>$ are two independent evidences, then the combination of E_1 and E_2 is
$E=<m_1 \oplus m_2, (VF_1+ VF_2)/2>$, where $\oplus$ is Dempster's rule of combination with value factors.

Mathematical Modelling

$S = \{T, N, D_S, I, C_M, R_R, R_T, I_R\}$
Where
T is Input and N, D_S, I, D_M, R_R, R_T, I_R are functionalities
T = Text Message N = Nodes
D_S = Data Sending I = Intrusion Recognition system
C_M = Choice Making R_R= Risk review
R_T = Routing Table alteration Detector
I_R = Intrusion Response
Nodes will be set of n nodes as follows
$N = \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8\}$ for n =8
$D_S= \{M, R\}$
Where M = Message & R = Route
I = {A, C}
Where A = Alert & C = Confidence Value
$C_M= \{R_E, R_T, T\}$
Where R_E=Risk Estimation R_T=Risk Tolerance T=Thresholds
$R_R= \{E, C\}$
Where E=Evidence & C=Countermeasure
$R_T= \{C_I, C_C\}$
Where C_I= Change Info, C_C= Change Count
$I_R= \{R_A, R_{TR}\}$
R_A= Response Actions, R_{TR}= Routing table recovery
Function Descriptor Table

Function	Function Description
F1	Nodes
F2	Data Sending
F3	Intrusion Recognition System
F4	Choice Making
F5	Risk review
F6	Routing Table alteration Detector
F7	Intrusion Response

Where
I1=Names & port number O1=Configured nodes
I2=Path & destination O2=Data send to destination
I3=Intrusion O3=Attack alert with confidence value
I4=Routing table O4=Count of changes on RT
I5=Alert Confidence & RTCD Information O5=$Risk_A$ & $Risk_C$
I6=Risk Estimation, Risk Tolerance & Thresholds

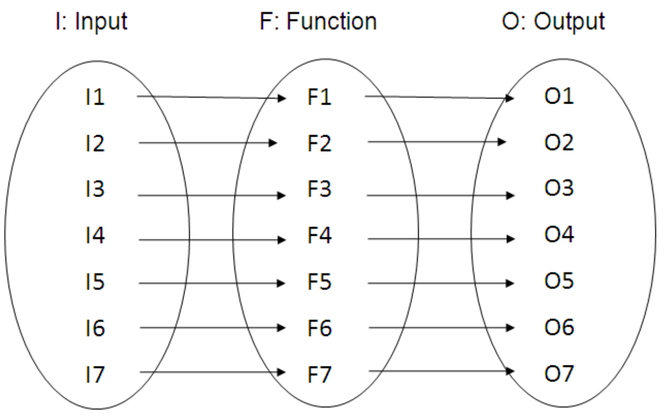


Fig. 2 Input Output of Functions

O6=choice
I7= $Risk_A$ and $Risk_C$ O7=RT recovery & Node Isolation

Algorithm for combination of multiple evidences

```
Algorithm 1. CME
INPUT: $E_P$ The Pool of Evidence
OUTPUT: One Evidence
$|E_P|$= sizeof ($E_P$)
While $|E_P|$ > 1 do
    Pick two evidences with least VF in $E_P$ named $E_1$ & $E_2$;
    Combine these two evidences,
    $E=<m_1 \oplus m_2, (VF_1+ VF_2)/2>$
    Remove $E_1$ & $E_2$ from $E_P$;
    Add E to $E_P$;
End
return the evidence in $E_P$
```

5. INTRUSION RESPONSE MECHANISM

In this section, Intrusion Response Mechanism is expressed based on quantitative risk estimation & quantitative risk tolerance. Instead of applying simple isolation of malicious nodes, this approach adopts an isolation mechanism in a temporal manner based on risk value. Risk review is performed with extended DS evidence theory for both attacks and corresponding countermeasures to make more precise response choice illustrated in Fig. 1.

Each node in the system formulates its own response choice based on the proofs & its personal individual benefits. Hence some nodes in MANET may separate the malicious node, but others may still be in cooperation with due to high dependency relationships. This Intrusion response mechanism is divided into the following steps as shown in Fig 1

Proof Gathering In this step Intrusion Recognition System (IRS) gives an attack alert with a confidence value, and then Routing Table Alteration Detector (RTAD) runs to figure out how many changes on routing table are caused by the attack.

Risk review Alert Confidence from Intrusion Recognition System, and the routing table altered information could be further considered as independent proofs for risk calculation and combined with the extended DS Theory. Risk of countermeasures is calculated as well during a risk review phase. Based on the risk of attacks & the risk of countermeasures, the entire risk of an attack could be figured out.

Choice Making The Adaptive Choice making module presents a flexible response decision-making mechanism, which takes risk estimation & risk tolerance into account. To

fine-tune temporary isolation level a user can set different thresholds to fulfill goals.

Intrusion Response by means of the output from risk review & choice making module, the corresponding response actions, including routing table recovery & node isolation, are carried out to lessen attack damages.

Selection of proofs/Evidences

Confidence level of alerts from Intrusion recognition System is considered as the subjective knowledge in Evidence 1. In terms of objective evidence different routing table modification cases are analyzed. There are three basic items in OLSR routing table (destination, next hop, distance). Thus routing attacks can cause existing routing table entries to be missed, or any item of routing table entry to be changed.

Evidence 1 Alert Confidence The confidence of attack recognition by the Intrusion Recognition System is provided to address the possibility of the attack occurrence. Since the false alarm is a serious problem, the confidence factor must be considered for the risk review of the attack. The basic probability assignments of Evidence 1 are based on three equations specified below:

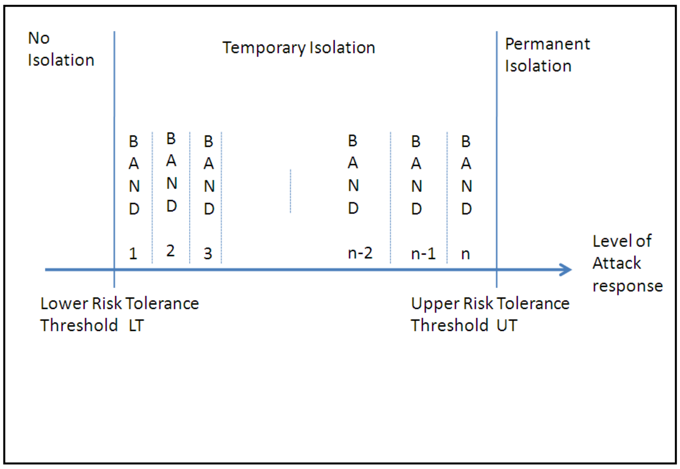
$m(Insecure) = C$, *C is confidence given by IRS* (5)

$m(Secure)=1-C$, (6)

$m(Secure, Insecure)=0$ (7)

Evidence 2 Missing Entry The evidence indicates the proportion of missing entries in routing table. Link with holding attack or node isolation countermeasures can cause possible deletion of entries from routing table of the node.

Evidence 3 Changing Entry I The evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case malicious node



builds a direct link to this node. So it is highly possible for this node to be the attacker's next target. Malicious node could drop all the packages to or from the target node, or it can behave as a normal node and wait for future attack actions. Note that isolating node cannot cause this case.

Evidence 4 Changing Entry II This evidence shows the proportion of changed entries in the case of different next hop (not the malicious node) and the same distance. Impacts on the node communication should be very minimal in this case. Both attacks and countermeasures could cause this case.

Evidence 5 Changing Entry III This evidence points out the proportion of changed entries in the case of different next hop (not the malicious node) & the different distance. Similar to Evidence 4, both attacks & countermeasures could result in this evidence. The path change may also affect routing cost and transmission delay of the network.

Combination of Evidences

For simplicity we call the combined evidence for an attack, E_A and the combined evidence for a countermeasure, E_C. Thus, $Bel_A(Insecure)$ and $Bel_C(Insecure)$ represent risk of attack ($Risk_A$) and countermeasure ($Risk_C$) respectively. The combined evidences E_A and E_C are defined in (8) and (9). The entire risk value derived from $Risk_A$ and $Risk_C$ is given in (10).

$E_A= E_1\oplus E_2\oplus E_3\oplus E_4\oplus E_5$ (8)

$Ec= E_2\oplus E_4\oplus E_5$ (9)

Where $\oplus$ is Dempster's rule of combination with Value factors

$Risk = Risk_A - Risk_C= Bel_A(Insecure)-Bel_C(Insecure)$ (10)

Adaptive Choice Making

Adaptive choice making module is based on quantitative risk estimation and risk tolerance, which is shown in fig 2. The response level is additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action. The response action and band boundaries are all determined in accordance with risk tolerance and can be changed when risk tolerance threshold changes. The upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would remain each node intact. The band between the upper tolerance threshold and lower tolerance threshold is associated with the temporary isolation response, in which the isolation time (T) changes dynamically based on the different response level. The value of lower risk tolerance threshold is 0 initially if no additional information available. It implies when risk of attack is greater than risk of isolation response, the isolation is needed. If other information is available, it could be used to adjust thresholds. For example node reputation is one of the important factors in MANET security. That is if compromised node has high or low reputation level the response module can intuitively adjust the risk tolerance thresholds accordingly.

6. RESULTS

By considering example Topology as shown in figure

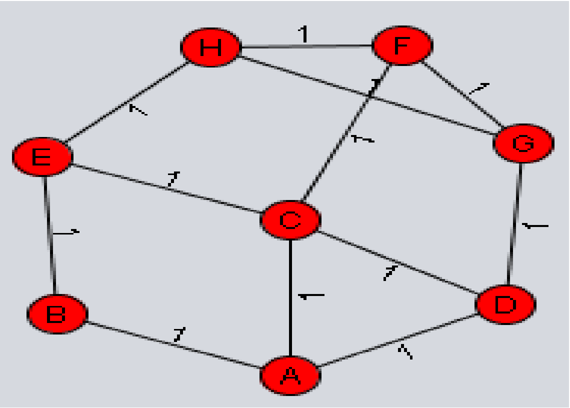


Fig.4 Example Scenario

Attack Link is generated B to G as follows

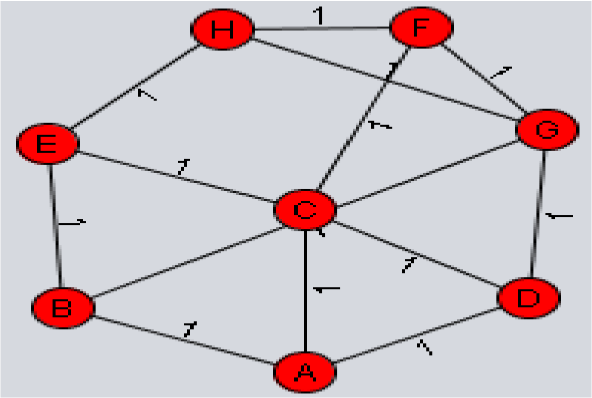


Fig.5 Attack Link Generation

After Isolation topology becomes as follows

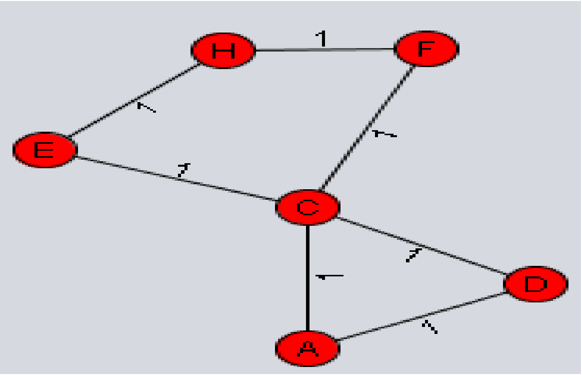
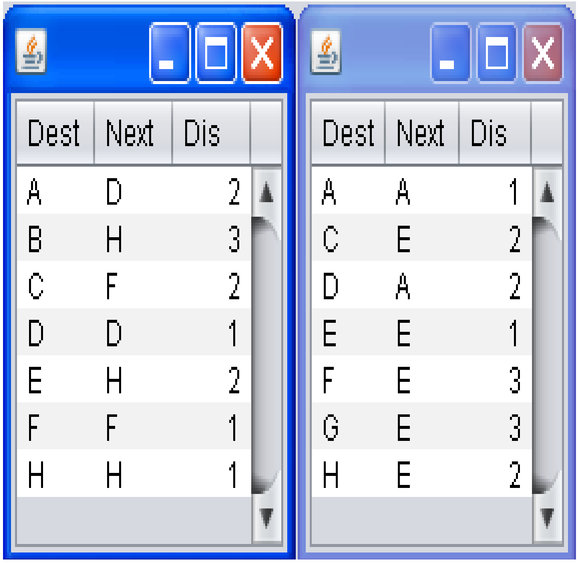


Fig.6 Isolation

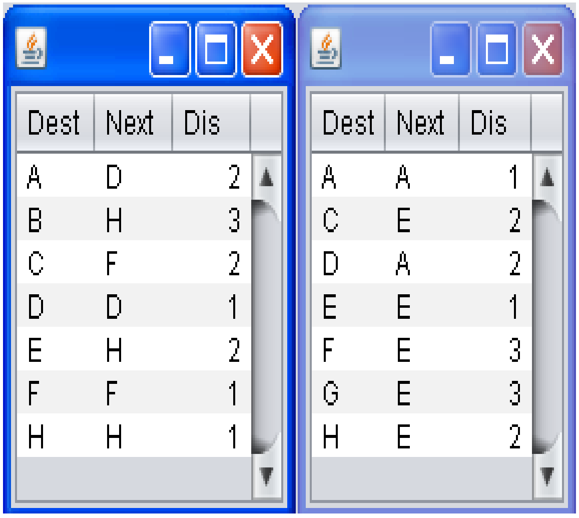
Routing tables of B & G nodes



Dest	Next	Dis
A	D	2
B	H	3
C	F	2
D	D	1
E	H	2
F	F	1
H	H	1

Dest	Next	Dis
A	A	1
C	E	2
D	A	2
E	E	1
F	E	3
G	E	3
H	E	2

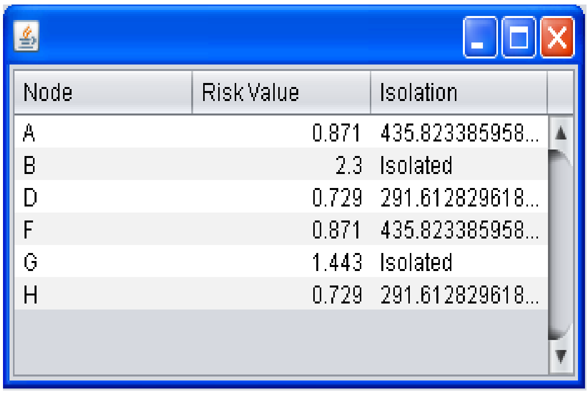
After attack Routing tables of B & G nodes



Dest	Next	Dis
A	D	2
B	H	3
C	F	2
D	D	1
E	H	2
F	F	1
H	H	1

Dest	Next	Dis
A	A	1
C	E	2
D	A	2
E	E	1
F	E	3
G	E	3
H	E	2

Total Risk value table calculated as follows



Node	Risk Value	Isolation
A	0.871	435.823385958...
B	2.3	Isolated
D	0.729	291.612829618...
F	0.871	435.823385958...
G	1.443	Isolated
H	0.729	291.612829618...

Fig.9 Total Risk values of nodes

7. CONCLUSION

Intrusion Response mechanism for routing attack in Mobile Ad hoc network is implemented. This approach considered the potential damages of attacks and countermeasures. In order to measure the risk of both attacks and countermeasures, Dempster Shafer Mathematical theory of Evidence is extended with a notion of value factors. With this, Nodes in MANET can have precise decision about No Isolation, temporary Isolation or Permanent Isolation which ultimately protects MANET from harmful immature response to routing attacks. Results and graphs clearly show improvement in packet delivery ratio by Dempster Shafer theory of evidence with Value factor

REFERENCES

[1] Zakirullah; Islam, M.H.; Khan, A.A. "Detection of dishonest trust recommendations in mobile ad hoc networks", *Computing, Communication and Networking Technologies (ICCCNT), 2014*

[2] Yingpu Zhu; Lu Liu; Panneerselvam, J.; Liangmin Wang; Zhiyuan Li "Credit-Based Incentives in Vehicular Ad Hoc Networks", *Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on,* On page(s): 352 – 357

[3] Abirami, K.R.; Sumithra, M.G.; Rajasekaran, J. "An enhanced intrusion detection system for routing attacks in MANET", *Advanced Computing and Communication Systems (ICACCS), 2013*

[4] Pakleppa, M.; Vorstius, J.B.; Keatch, R.; Tapia-Siles, S.C.; Coleman, S.; Cuschieri, A. "Dempster-Shafer theory applied in state estimation of a pressure driven endoscope for Hydro-colonoscopy", *Information Fusion*

[5] *(FUSION), 2013 16th International Conference on,* On page(s): 1413 - 1420, Volume: Issue: , 9-12 July 2013

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

[7] 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.

[8] M. Yamada and M. Kudo, "Combination of Weak Evidences by D-S Theory for Person Recognition," Knowledge-Based Intelligent Information and Engineering Systems, pp.1065-1071,Springer,2004.

[9] 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

[10] 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,May2010.

[11] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol.11, no.1, pp.21-38, 2005.

[12] B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols(ICNP'02), pp.78-88,2002.

[13] Y.Hu, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, vol.1, no.1, pp.175-192, 2003.

[14] B. Awerbuch, R .Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks," ACMTrans. Information and System Security, vol.10,no.4,pp.1-35,2008.

[15] 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),pp.330-350,2006.

[16] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom,pp.255-265,2000.

[17] 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,pp.65-68,2006.

[18] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, vol.3,pp.1976-1986,2004.

[19] 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.

[20] 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), pp.388-391,2009.

[21] 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.

[22] 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.

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

[24] A. Jaganraj, A. Yogaraj, N. Vignesh, R. V. Anuroop, "

[25] Handling MANET routing attacks using risk aware mitigation mechanism with distributed node control".

[26] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu,

[27] "Risk-Aware Response for Mitigating MANET Routing Attacks."

[28] Sudarshan Phule, G. T. Chavan "Intrusion Response with Dempster Shafer theory of evidence to detect and overcome routing attack in Mobile Ad hoc Networks" Cpgcon 2015

BIOGRAPHIES

Sudarshan Phule is currently pursuing M.E. in Sinhgad College of Engineering Savitribai Phule Pune University.

G. T. Chavan is currently working towards PhD degree & working in Sinhgad College of Engineering Savitribai Phule Pune University.