ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Effective Intrusion Reduction in Manet

B. Hariprasad[1]
M.Tech 2nd year, Dept. of CSE
SITE Engg. College
Andhrapradesh, India

Sri A. Narayanarao[2]
Asso.prof, Dept. of CSE
SITE Engg. College
Andhrapradesh, India

Sri. O. Devakiran[3]
Asso.prof, Dept. of CSE
SITE Engg. College
Andhrapradesh, India

Abstract: ***The main challenges in Mobile Ad hoc Networks (MANET) is to design the robust security solution that can protect MANET from various routing attacks. In the presence of malignant nodes, routing causes the most destructive harms to MANET. Even though there available several intrusion response techniques to control such negative attacks, existing solutions typically attempt to isolate malignant nodes based on binary or naive fuzzy response decisions. However, binary responses make additional harms to the network infrastructure by unexpected network partition, causing, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, we propose a hazard detection response mechanism to systematically deal with the identified routing attacks. Our proposed methodology is focused around an augmented Dempster-Shafer scientific hypothesis of confirmation presenting an idea of essentialness variables. Moreover, our tests show the viability of our methodology with the attention of a few execution measurements.***

Keywords: MANET, Mobile Ad hoc Networks, D-S Theory, Intrusion Response, Hazard Detection, Risk Aware

I. INTRODUCTION

A mobile ad hoc network (MANET) is an outlining toward oneself system that is framed consequently by an accumulation of portable hubs without the assistance of an altered framework or unified administration. Every node is furnished with a remote transmitter and recipient, which permit it to correspond with different nodes in its radio correspondence range. Dynamic Nature is MANET's Special normal for its system topology which would be often changes because of the capricious versatility of node. Every node assumes a switch part in MANET while transmitting information over the system. In place for a node of forward a packet to a node that is out of its range, the participation of different nodes in the system is required; this is known as multi-hop correspondence. There for every node must go about as both a host and a switch in the meantime. As Manets get to be broadly utilized, the security has turned into one of the essential concerns. For instance, the vast majority of the steering conventions proposed for Manets accept that each node in the system is agreeable and not dangerous. In this way, one and only bargained node can result in the disappointment of the whole system.

A few interruption recognition frameworks produce reactions in MANET by isolating uncooperative hubs focused around the notoriety got from their disposition. Such basic arrangements against threatening node leads reactions. In MANET situation, despicable countermeasures may lead the unpredicted system division, brining extra harm to the system framework.

The thought of the danger can be received to backing more versatile reactions to directing assaults in MANET. The danger evaluation is still genuine testing issue because of its associations of subjective information, target proof and intelligent thinking. Subjective knowledge could be recovered from past experience and from perception objective reasoning could be acquired while legitimate thinking needs a formal establishment. [4] A naïve fuzzy cost-sensitive intrusion response solution intended for MANET just by considering subjective knowledge and objective reasoning. In a subjective knowledge

administration model with various choice elements focused around the methodology hypothesis and the fluffy rationale tenets expectation system Afstrust are utilized. The primary tangles are fluffy reactions could result in to uncertainity in directing assaults countering in MANET and they can't ascertain a precise limit esteem for every node.

In [2],to control the asset use among all hubs and augment the lifetime of a MANET, hubs with the most exceptional assets ought to be choosen as the pioneers. The downsides are positions to empower hubs in partaking genuinely in the pioneer decision process and structures a brought together control.

In [3], a versatile rank administration framework understood that redesigns in system conditions reason changes in node conduct and that adjusts to such changes by suit its working parameters. The recognition module can utilize a SPRT (Sequential Probability Ratio Test) to separate operative and uncooperatie neighbors. The impediments are if the most brief way having the risk client then it is not considered as course and no disengagement of node.

In [4],a class of persistent measurements to assess the helplessness of system movement as a capacity of security and directing conventions utilized as a part of remote systems. The measurements and hub catch assaults utilizing the GNAVE algorithm. The impediments are it chiefly concentrate on hub catch assault and the GNAVE algorithm being avaricious intimates that the assault execution depends just on the request of the weighted node values for the nodes.

These instabilities holes are satisfied by utilizing Dempster-More secure scientific hypothesis of proof (D-S hypothesis). D-S hypothesis has a few attributes. To start with, it empowers us to speak to both subjective and target confirmations with fundamental likelihood task and conviction capacity. Second, it backings proves together with plausible thinking. Dempster's guideline of mix with an idea of significance elements (IF) in D-S confirmation model settles the needs and separation limits among treating proofs.

In this paper we proposed a viable interruption identification and reaction instrument to efficiently code with directing assaults in MANET. We done a succession of reenacted tests on MANET's proactive directing convention, OSLR(Optimized link State Routing Protocol)[12]. The fundamental associations of this paper are abridged as takes after:

- » We formally proposed a nonassociative and weighted significance components with D-S evidence model.
- » Harms brought about by both assaults and countermeasures are considering our proposed model by a versatile danger location and reaction instrument with augmented D-S evidence model.
- » We asses our reaction component in position to agent assault situations and tests. Yields unmistakably demonstrate the viability and adaptability of our propose approach.

Whatever is left of the paper is composed as takes after: area 2 reviews an OSLR MANET routing convention and steering assaults in position to OSLR. Area 3 depicts how out developed D-S evidence model can be incorporate with significance elements. Area 4 shows the points of interest of our propose response mechanism. The assessments of our approach are discussed in section 5. Section 6 provides the work related to MANET intrusion detection and response systems, also reviews hazard awareness approaches in difference fields. Section 7 concludes this paper.

II. Routing Protocols And Attacks

The Simulation modeling has turned into a supportive device for comprehension the action of MANET. This is because of behavior of the network. During the recent years, determination of enhanced routes from a source to some end in Ad hoc network is considered adequately and different routing protocols were likewise created. The transmission extent is restricted and hence the information transmission between the two nodes can be made utilizing various hops. The circumstances gets to be more terrible because of the mobility of the distinctive hubs. The accompanying peculiarities are crucial for a convention to be utilized as a part of the Ad Hoc system:

» Adaptation of topology changes is vital for the protocol and it ought to likewise give Loop free routing.

» The blockage issue can be controlled by the protocol by giving different routes from the source to end of the line.

» The trade of routing data causes topology changes to happen, so the protocol ought to have negligible control messages.

» The protocols may get to be invalid after at some point, so it must be took into account brisk foundation of routes

a) Routing protocols terminology :

The data about the connecting node and neighbors are kept up by the routing table created by the routing protocol. Both the wired and wireless networks comprise of a few routing protocols which are ordered into four different classes focused around their properties.

Centralized Vs. Distributed

The route choice for centralized algorithms and distributed algorithms are diverse. Determination is made at focal node in centralized algorithm while, in the later algorithm the choice of route is imparted among the network nodes.

Static Vs. Adaptive

The route utilized by source destination combines as a part of the static algorithm is settled being autonomous of movement conditions. The node or connection disappointment reaction is considered for the change of the route for moves. In a wide mixture of activity information designs, high throughput can't be accomplished by these calculations. The significant packet network changes the route between the source and the terminus since it utilizes a adaptive routing.

Flat Vs. Hierarchical

A flat routing approach can be made by the flat addressing. Every last node in the routing is mindful as it assumes a real part and no unique nodes are considered. Hierarchical routing is very not the same as the flat as it gives obligation regarding each one network node independently. Proactive Vs Reactive Vs Hybrid

The Ad-hoc routing protocols are classified as follows.

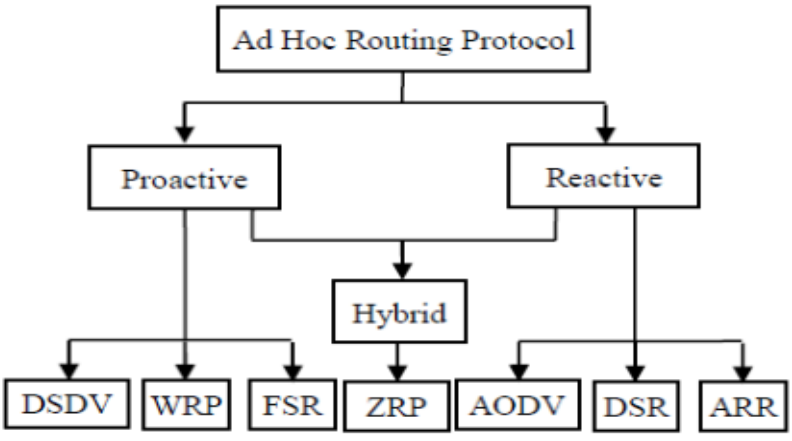


Fig 1. Classification of Routing Protocols

b) Classification Of Attacks :

Offering security to the Mobile Ad-hoc Network is a troublesome undertaking. To given better answer for security attack, First we must distinguish and see about the attack. As a result of the inaccessibility of incorporated organizer in MANET, the security is a testing undertaking in wireless communication. The security attack classification is given underneath:

The threats for MANETs are classified as follows.

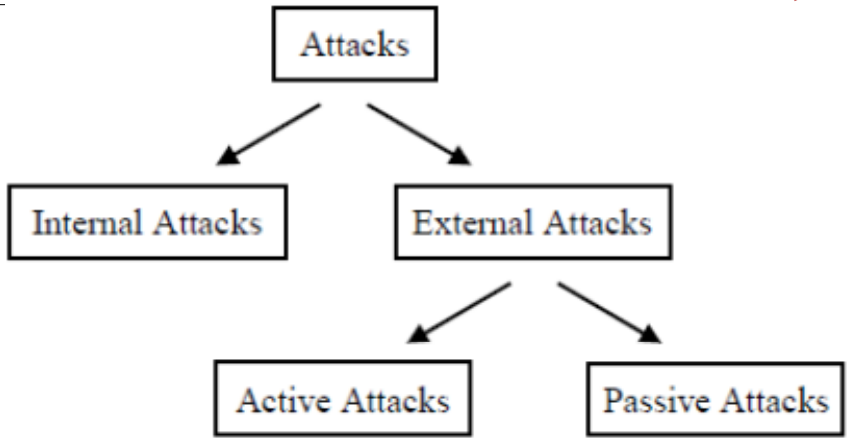


Fig 2. Attacks classification

a. Internal Attack: The internal attacks are launched from the bargained nodes in the mobile Ad-hoc network. In here the attacker node gets the unapproved get to and demonstrating that as a typical portable node. It examinations the information streams between the nodes in the network.

b. External Attack: These attacks are made by the nodes that are outside the network. It makes wrong routing data or administration inaccessibility.

The External Attacks have two different classifications. They are:

» Active Attack

» Passive Attack

Active Attacks:

The active attacks are hurtful one this attacks keep the information streams between the source and end of the line nodes. This active attack either may be inside or outside. The active outer attacks made by the nodes which fit in with the outside of the network. The internal attacks are more destructive and hard to locate. This inside active attacks are made by the malignant nodes which are has a place with the network. These attacks are more upheld for the assailants to alter the information packets and that makes the congestion in the network. In here the malignant node change the routing data and publicize its wrong routing path as the best routing way.

Passive attacks:

The passive attack does not make any progressions in the rouging information packet. It simply screens the system movement. It doesn't influence the routing protocol operation however listen the protocol's routing usefulness. With a specific end goal to dodge this sort of attacks we require solid encryption and decryption algorithms for information transmission.

III. D-S Theory of Evidence

The Dempster–Shafer theory (DST) is a mathematical theory of evidence. It allows one to combine evidence from different sources and arrive at a degree of belief (represented by a belief function) that takes into account all the available evidence. The theory was first developed by Arthur P. Dempster and Glenn Shafer. Dempster's 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.

» ***Associative:***

For DRC , the order of the information in the aggregated evidences does not impact the result. As shown in [10], a non associative combination rule is necessary for many cases.

» ***Nonweighted.***

DRC implies that we trust all evidences equally [11]. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence.

Yager [10] and Yamada and Kudo [18] proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. [11] suggested a weighted combination rule to handle the second 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 and criticality. Our extended Dempster-Shafer theory with *importance factors* can overcome both of the aforementioned limitations.

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*.

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

Definition 2. An evidence E is a 2-tuple (X,IF), where X describes the basic probability assignment [5]. Basic probability assignment function X is defined as follows:

$$X(\text{ø})=0 \quad (1)$$

And $$\sum_{A\subseteq\Theta} X(A)=1 \quad (2)$$

According to [5], a function $Bl:2^{\Theta}\rightarrow[0,1]$ is a belief function over Θ if it is given by (3) for some basic probability assignment x: $2^{\Theta}\rightarrow[0,1]$

$$\text{Bl(A)}=\sum_{B\subseteq A} X(B) \quad (3)$$

For all $A\in 2^{\Theta}$, Bl(A) describes a measure of the 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's rule of combination, which is given by (4), enables us to compute the orthogonal sum, which describes the combined evidence.

Suppose Bl1 and Bl2 are belief functions over the same frame Θ, with basic probability assignments x1 and x2. Then, the function x: $2^{\Theta}\rightarrow[0,1]$ defined by X(ø)=0 and

$$X(C)=\frac{\sum_{Ai\cap Bj=C} X_1(A_i)X_2(B_j)}{1-\sum_{Ai\cap Bj=\phi} X_1(A_i)X2(B_j)} \quad (4)$$

For all nonempty $C\subseteq\Theta$, X(C) is a basic probability assignment which describes the combined evidence.

Suppose IF_1 and IF_2 are *Importance 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 evidences is less than 1. This is straightforward since if our belief to one evidence is 1, it would mean our belief to the other is 0, which models a meaningless evidence. And we define the *importance factors* of the combination result equals to $(IF_1+IF_2)/2$

Definition 3: Extended D-S evidence model with *importance factors*: suppose $E_1 = \langle x_1, IF_1 \rangle$ $E_2 = \langle x_2, IF_2 \rangle$ are two independent evidences. Then the combination of E1 and E2 is $E = \langle X_1 \oplus X_2, (IF_1 + IF_2)/2 \rangle$ where $\oplus$ is Dempster's rule of combination with *importance factors*.

1) *Expected Properties for Our Dempster's Rule of Combination with Importance Factors*

The proposed rule of combination with *importance factors* should be a superset of Dempster's rule of combination. In this section, we describe four properties that a candidate Dempster's rule of combination with *importance factors* should follow. Properties 1 and 2 ensure that the combined result is a valid evidence. Property 3 guarantees that the original Dempster's rule of combination with *importance factors*, where the combined evidences have the same priority. Property 4 ensures that *importance factors* of the evidences are also independent from each other.

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

$$X'(\phi) = 0 \tag{5}$$

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

$$\sum_{A \subseteq \Theta} X'(A) = 1 \tag{6}$$

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

$$X'(A, IF_1, IF_2) = X(A), \text{ if } IF_1 = IF_2 \tag{7}$$

For a $A \in \Theta$,where X(A) is the original Dempster's Combination Rule.

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

$$X'(A, IF_1, IF_2) \neq X'(A, IF_2, IF_1) \text{ if } IF_1 \neq IF_2 \tag{8}$$

2) *Dempster's Rule of Combination with Importance Factors*

In this section, we propose a Dempster's rule of combination with importance factors. We prove our combination rule follows the properties defined in the previous section.

Theorem 1. Dempster's Rule of combination with Importance Factors: Suppose Bl1 and Bl2 are belief functions over the same frame of discernment Θ, with basic probability assignment x1 and x2. The importance factors of these evidences are IF1 and IF2. Then the function $X' : 2^{\Theta} \to [0,1]$ defined by

$$X'(\phi) = 0$$

and

$$X'(C, IF_1, IF_2) = \frac{\sum_{A_i \cap B_j = C} [X_1(A_i)^{\frac{IF_1}{IF_2}} . X_2(B_j)^{\frac{IF_2}{IF_1}}]}{\sum_{C \subseteq \Theta, C \neq \phi} \sum_{A_i \cap B_j = C} [X_1(A_i)^{\frac{IF_1}{IF_2}} . X_2(Bj)^{\frac{IF_2}{IF_1}}]}$$

for all nonempty $C \subseteq \Theta$, X' is a basic probability assignment which describes the combined evidence.

Proof. It is obvious that our proposed DRCIF holds properties 1 and 4. We prove that our proposed DRCIF also holds properties 2 and 3 here.

Property 2.

$$\sum_{A\subseteq\Theta} X'(A, IF_1, IF_2) =$$

$$\sum_{A\subseteq\Theta, A\neq\phi} \frac{\sum_{A_i\cap B_j=A}[X_1(A_i)^{\frac{IF_1}{IF_2}}.X_2(B_j)^{\frac{IF_2}{IF_1}}]}{\sum_{A\subseteq\Theta, A\neq\phi}\sum_{A_i\cap B_j=A}[X_1(A_i)^{\frac{IF_1}{IF_2}}.X_2(B_j)^{\frac{IF_2}{IF_1}}]}$$

$$= \frac{\sum_{A\subseteq\Theta, A\neq\phi}\sum_{A_i\cap B_j=A}[X_1(A_i)^{\frac{IF_1}{IF_2}}.X_2(B_j)^{\frac{IF_2}{IF_1}}]}{\sum_{A\subseteq\Theta, A\neq\phi}\sum_{A_i\cap B_j=A}[X_1(A_i)^{\frac{IF_1}{IF_2}}.X_2(B_j)^{\frac{IF_2}{IF_1}}]} = 1$$

Property 3.

$$X'(A, IF_1, IF_2)$$

$$= \frac{\sum_{A_i\cap B_j=A}[X_1(A_i)^{\frac{IF_1}{IF_2}}.X_2(B_j)^{\frac{IF_2}{IF_1}}]}{\sum_{A\subseteq\Theta, A\neq\phi}\sum_{A_i\cap B_j=A}[X_1(A_i)^{\frac{IF_1}{IF_2}}.X_2(B_j)^{\frac{IF_2}{IF_1}}]}$$

$$= \frac{\sum_{A_i\cap B_j=A}[X_1(A_i)\ .X_2(B_j)\ ]}{\sum_{A\subseteq\Theta, A\neq\phi}\sum_{A_i\cap B_j=A}[X_1(A_i)\ .X_2(B_j)\ ]}$$

$$= \frac{\sum_{A_i\cap B_j=A}[X_1(A_i)\ .X_2(B_j)\ ]}{1-\sum_{A_i\cap B_j=\phi}[X_1(A_i)\ .X_2(B_j)\ ]} = X(A)$$

Our propose DRCIF is non associative for multiple evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm, supports this requirement and the complexity of our algorithm is O(n), where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naïve fuzzy-based method. The algorithm for combination of multiple evidences is constructed as follows:

Algorithm 1: CMB-OF-MULP-EVDS

Input : Evidences pool EVp

Output: One evidence

|EVp|=sizeof(EVp);

While |EVp|>1

Get evidences pair with the least IF in EVp

Named E_i and E_j;

Combine these pair evidences,

$$E = \langle X_1 \oplus X_2, (IF_1 + IF_2)/2 \rangle ;$$

Remove E_i and E_j from EVp;

Add E to EVp

End while

Return the evidence in EVp

IV. Hazard Detection And Response Mechanism

In this Section, we express a versatile Danger discovery and reaction system focused around quantitative danger estimation and issue resistance. As opposed to applying basic parallel disengagement of harmful nodes, our methodology receives a detachment instrument in a transient way focused around the danger esteem. We perform Danger appraisal with the expanded D-S evidence hypothesis presented in section 3 for both attacks and comparing countermeasures to settle on more exact response choice in fig 1.

a) Overview

On account of the framework less architecture of MANET our hazard discovery and response mechanism is circulated, which implies every node in this framework settles on its own response decisions focused around the confirmations and its own particular individuals advantages. In this way, a few nodes in MANET may isolate the dangerous node, yet others may in any case keep in collaboration with because of high reliance connections. Our risk recognition and response mechanism is partitioned into the accompanying four steps demonstrated in fig 1.

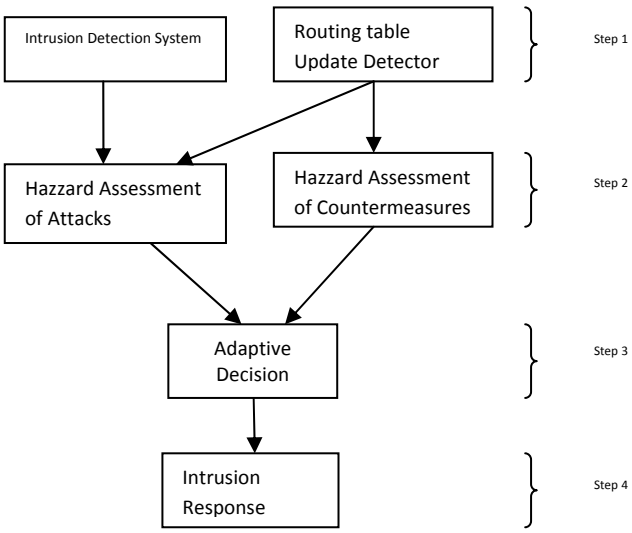


Fig 3. Architecture

Evidence Gathering. In this step Intrusion Detection System(IDS) gives an assault alarm with a certainty worth, and afterward Routing Table Change Detector (RTCD) hurries to make sense of what number of changes on steering table are brought about by the assault.

Hazard Assessment. Caution certainty from IDS and the routing table changing data would be further considered as autonomous evidences for danger calculation and joined with the extended D-S hypothesis. Danger of countermeasures is ascertained also amid a danger evaluation stage. Taking into account the danger of assaults and the danger of countermeasures, the whole danger of an assault could be made sense of.

Decision Making. The adaptive decision module gives an adaptable response decision making mechanism, which considers hazard estimation and danger resistance. To modify temporary isolation level, a user can set diverse limits to satisfy her objective.

With the yield from danger evaluation and decision making module, the corresponding response actions, including routing table recuperation and node isolation, are completed to mitigate attack harms in a dispersed way

b) Response to Routing Attacks

In our methodology, we utilize two separate reactions to manage distinctive assault strategies: Routing table recuperation and node seclusion. Routing table recuperation incorporates nearby steering table recuperation and global routing recuperation. Nearby routing recuperation is performed by victimized person nodes that catch the assault and naturally recuperate its own routing table. Global routing recuperation includes with sending recouped routing messages by exploited person hubs and overhauling their steering table focused around remedied routing data progressively by different nodes in MANET. Directing table recuperation is a basic reaction and ought to serve as the first response system after effective location of assaults. In proactive steering conventions like OLSR, routing table recuperation does not bring any extra overhead since it intermittently runs with directing control messages. Likewise, the length of the discovery of assault is sure, this response causes no negative effects on existing routing operations.

Node isolation may be the most instinctive approach to keep further assaults from being dispatched by harmful nodes in MANET. To perform a node detachment node, the neighbors of the threatening hub overlook the harmful hub by not one or the other sending packets through it nor tolerating any packets from it. Then again, a paired hub segregation reaction may bring about negative effects to the routing operations, actually bringing more routing damages than the assault itself.

For example, in Fig. 4, Node 3 behaves like a malignant node. However, if every other node simply isolate Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanism are required. In our hazard detection response mechanism, we adopt two types of time-wise isolation responses: temporary isolation and *permanent isolation*, which are discussed in Section 4.4.

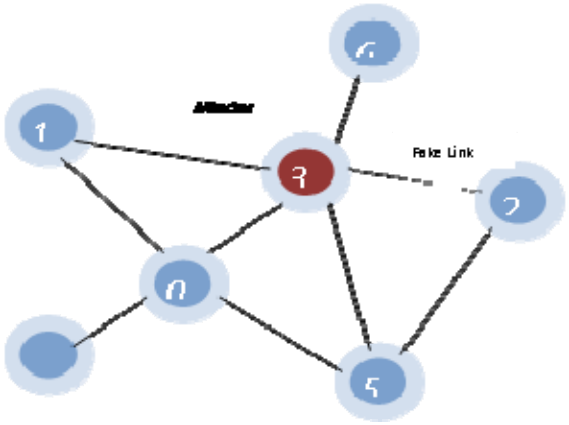


Fig. 4 Sample Manet

c) Hazard Assessment

Since the assault reaction activities may cause a bigger number of damages than assaults, the hazards of both assault and reaction ought to be evaluated. We arrange the security conditions of MANET into two classifications: {secure, Insecure}. At the end of the day, the edge of insight would be {ø, {secure}, {insecure}, {secure, Insecure}}. Note that {secure, Insecure} implies the security condition of MANET could be either secure or insecure, which depicts the instability of the security state. Bl{insecure} is utilized to represent to the danger of MANET

1) Selection of Evidences

Our evidence selection methodology considers subjective evidence from masters' information and objective evidence from routing table adjustment. We propose an unifiedanalysis approach for assessing the dangers of both assault *(HA)* and countermeasure *(HC)*.

We take the certainty level of alarms from IDS as the subjective knowledge in evidence 1. Regarding objective evidence, we break down distinctive routing table change cases. There are three essential things in OLSR routing table (goal, next hop, distance). In this manner, routing assault can result in existing routing table sections to be missed, or any thing of a routing table section to be changed. We outline the conceivable instances of routing table change and investigate the degrees of harm in evidences 2 through 5.

Evidence 1: Alarm certainty. The certainty of assault discovery by the IDS is given to address the likelihood of the assault event. Since the false alert is a genuine issue for most IDSs, the certainty element must be considered for the danger appraisal of the assault. The essential likelihood assignments of Evidence 1 are focused around three comparisons given underneath:

X(Insecure)= c; c is confidence given by IDS (9)

X(Secure) = 1-c (10)

X(Secure; Insecure)=0. (11)

Evidence 2: Missing section. This confirmation shows the extent of missing entrances in excursion table. Connection withholding assault or node disconnection countermeasure can result in conceivable erasure of entrances from directing table of the node.

Evidence 3: Changing entrance I. This evidence represents to the extent of changing passages on account of next hop being the threatening node. For this situation, the threatening node fabricates an immediate connection to this node. Thus, it is very workable for this node to be the assailant's target. Threatening node could drop all the packets to or from the target node, or it can carry on as an ordinary node and wait for future assault activities. Note that isolating a dangerous node can't trigger this case.

Evidence 4: Changing entrance II. This proof demonstrates the extent of changed sections on account of distinctive next hop (not the threatening node) and the same separation. We accept the effects on the node correspondence ought to be extremely insignificant for this situation. Both assaults and countermeasures could result for this situation.

Evidence 5: Changing passage III. This proof brings up the extent of changing passages on account of diverse next hop (not the dangerous node) and the same distance. Like Evidence 4, both assaults and countermeasures could bring about this proof. The way change might likewise influence routing expense and transmission deferral of the system.

Fundamental likelihood assignments of proofs 2 to 5 are focused around (12-14). Comparisons (12-14) are piecewise direct capacities, where a,b,c and d are constants and controlled by specialists. D is the base estimation of the conviction that suggests the status of MANET is frail. Then again, 1-d is the most extreme estimation of the conviction that implies the status of MANET is secure. a,b and c are the edges for least conviction or most extreme conviction for every separate mass function

$$X(insecure)=\begin{cases} d & y\in[0,a] \\ (\frac{1-2d}{c-a})(y-a) & y\in(a,c] \\ 1-d & y\in(c,1] \end{cases} \quad (12)$$

$$X(secure)=\begin{cases} 1-d+(\frac{2d-1}{b})y & y\in[0,b] \\ d & y\in(b,1] \end{cases} \quad (13)$$

$$X(Secure, Insecure) = \begin{cases} \frac{1-2d}{b} y & y \in [0, a] \\ d - \frac{2d-1}{b} y - \frac{1-2d}{c-a}(y-a) & y \in (a, b] \\ 1 - b - \frac{1-2d}{c-a}(y-a) & y \in (b, c] \\ 0 & y \in (c, 1] \end{cases} \quad (14)$$

2) Combination of Evidences

For simplicity, we call the combined evidences for an attack, EA and the combined evidence for countermeasure, Ec. Thus, BlA(Insecure) and Blc(Insecure) represent risks of attack ($_{HA}$) and countermeasure($_{HC}$), respectively. The combined evidences, EA and EC are defined in (15) and (16). The entire risk value derived from $_{HA}$ and $_{HC}$ is given in (17)

$$E_A = E_1 \oplus E_2 \oplus E_3 \oplus E_4 \oplus E_5, \quad (15)$$

$$E_C = E_1 \oplus E_4 \oplus E_5, \quad (16)$$

Where $\oplus$ is Dempster's rule of combination with important factors defines in theorem1.

$$Hazzard = H_A - H_C = Bl_A(Insecure) - Bl_C(Insecure) \quad (17)$$

3) Adaptive Decision Making

Our adaptive decision-making module is focused around quantitative danger estimation and danger resilience, which is demonstrated in Fig. 3. The reaction level is furthermore separated into different groups. Each one band is connected with a isolation degree, which exhibits an alternate time of the isolation activity. The reaction activity and band limits are all decided as per danger resilience and can be changed when hazard resistance limit changes. The upper danger resilience limit (UT) would be connected with lasting separation reaction. The lower hazard resilience limit (LT) would stay every node in place. The band between the upper resistance edge and lower resilience limit is connected with the transitory disconnection reaction, in which the seclusion time (T) changes alertly focused around the distinctive reaction level given by (18) and (19), where n is the quantity of groups and i is the relating confinement band

$$i = \left\lceil \frac{Hazzard - LT}{HT - LT} \times n \right\rceil, Hazzard \in (LT, HT), \quad (18)$$

$$T = 100 \times i \text{ (milliseconds)}. \quad (19)$$

We prescribe the estimation of lower danger resilience limit be 0 at first if no extra data is accessible. It suggests when the danger of assault is more noteworthy than the danger of disengagement reaction, the isolation is required. On the off chance that other data is accessible, it could be utilized to conform edges. For instance, node notoriety is one of essential components in MANET security, our adaptive decision making module could consider this element also. That is, if the bargained node has a high or low notoriety level, the reaction module can naturally modify the danger resilience limits likewise. For the situation that LT is short of what 0, regardless of the fact that the danger of assault is not more prominent than the danger of segregation, the reaction could likewise perform a isolation errand to the dangerous nodes.

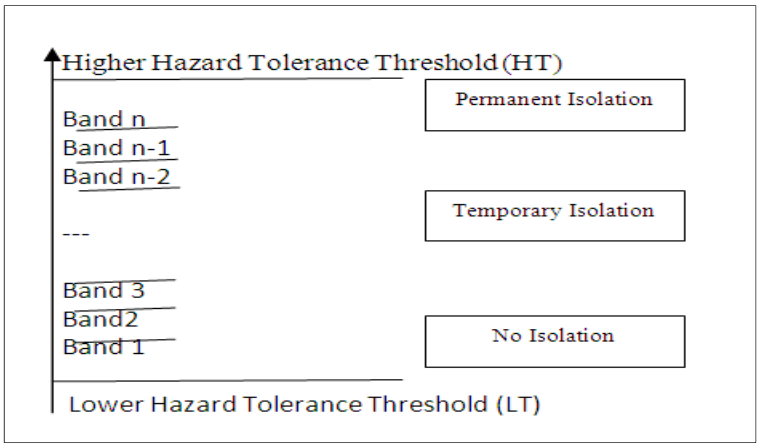


Fig. 5. Adaptive Decision Making

The danger resistance limits could likewise be alterably balanced by an alternate components, for example, assault recurrence. On the off chance that the assault recurrence is high, more extreme reaction move ought to be made to counter this assault. Our hazard detection response module could accomplish this goal by lessening the estimations of danger resistance edge and narrowing the reach between two danger resilience limits.

V. CASE STUDY

In this section, we first explain the methodology of our experiments and the metrics considered to evaluate the effectiveness of our approach. Then, we demonstrate the detailed process of our solution with a case study and also compare our hazard detection approach with binary isolation. The results show the effectiveness and scalability of our approach.

a) Methodology and Metrics

The examinations were completed utilizing NS-2 as the reproduction device from VINT Venture [19] with UM-OLSR [20]. NS-2 is a discrete occasion system test system which gives an itemized model of the physical and connection layer conduct of a remote system and permits subjective development of hubs inside the system. UM-OLSR is a usage of Upgraded Connection State routing convention for the NS-2, which consents to [12] and backings all center functionalities of OLSR in addition to the connection layer input alternative. In our trials, we built MANET situations in a topology of 1;000 m _ 1;000 m range. The aggregate reproduction time was situated to 1,200 seconds, and the transfer speed was situated to 2 Mbps. Consistent Bit Rate CBR) activity was utilized to send 512 byte-UDP packets between nodes. The lining limit of each hub was situated to 15. We embraced an irregular activity generator in the recreation that picked arbitrary sets of nodes and sent packets between them. Each node stayed informed regarding all packets sent independent from anyone else and the whole packet got from different nodes in the system. So as to assess the viability of our adaptive peril recognition reaction arrangement, we partitioned the recreation process into three stages and looked at the system execution as far as six measurements. The accompanying portrays the exercises connected with each one stage:

Stage 1: preceding assault. Arbitrary parcels were created and transmitted among nodes without actuating any of them as aggressors. This reproduction can show the activity designs under the ordinary situation.

Stage 2: After assault. Particular hubs were situated as aggressors which directed harmful exercises for their own particular benefits. On the other hand, any recognition or reaction is not accessible in this stage. This reproduction procedure can introduce the movement designs under the situation with dangerous exercises.

Stage 3: after reaction. Reaction choices for every node were made and completed focused around three separate instruments. We figured six measurements [21] for every reenactment run:

» Packet delivery radio. The proportion between the quantity of packets started by the application layer CBR sources and the quantity of packets got by the CBR sink at the last destination.

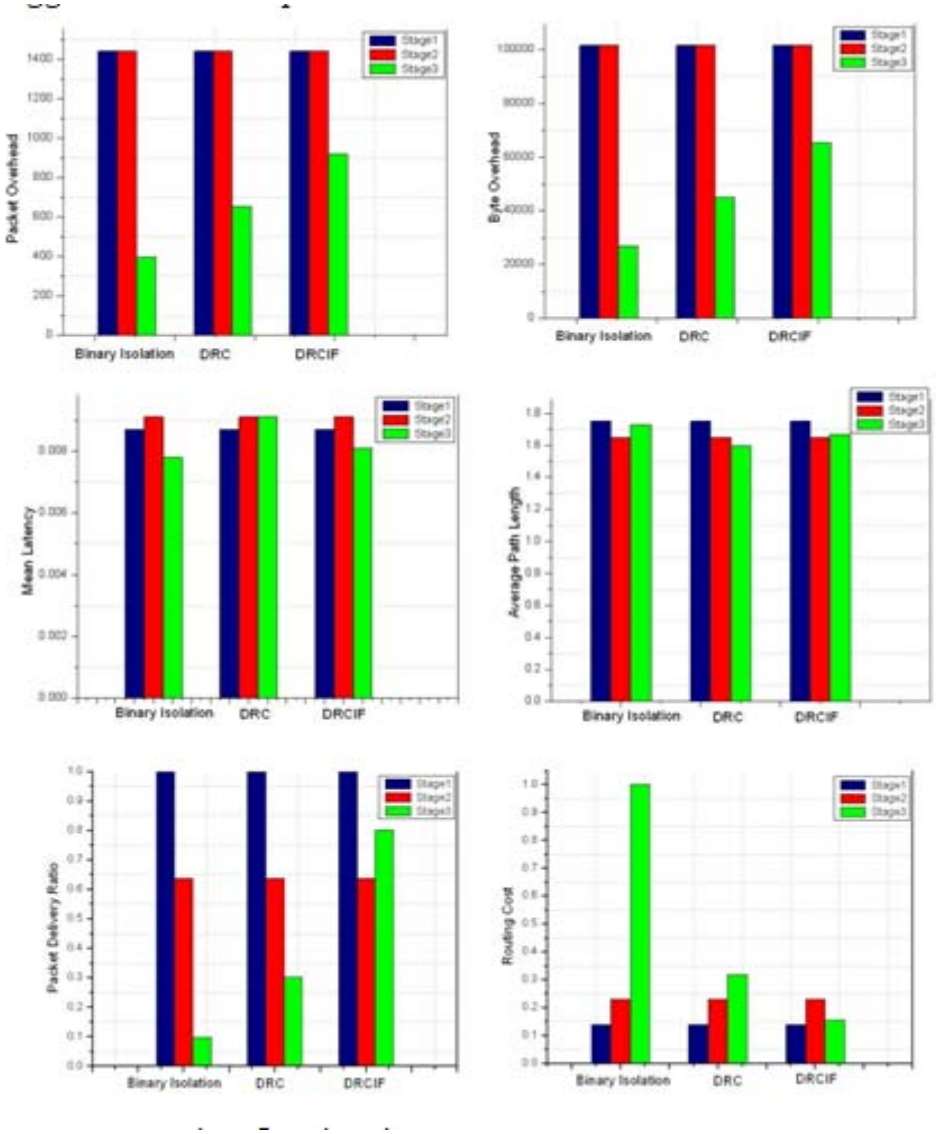
» Routing Cost. The degree between the aggregate bytes of routing packets transmitted amid the reproduction and the aggregate bytes of packets got by the CBR sink at the last end of the line.

» Packet overhead. The quantity of transmitted routing packets; for instance, a Welcome or TC message sent in excess of four hops would be included as four packets this metric.

» Byte overhead. The quantity of transmitted bytes by routing packets, numbering each one bounce like packet Overhead.

» Mean latency. The normal time passed from "when an information packet is first sent" to "when it is initially gotten at its end."

» Average Path length. This is the normal length of the ways found by OLSR. It as ascertained by averaging the quantity of bounces taken by every information packet to achieve the objective.



b) Case Study

Fig. 2 demonstrates our research endeavor situation, where packets from nodes 1 to 2 should experience nodes 0 and 5. Assume a harmful node 3 publicizes it has an immediate connection (fake connection) to node 2 and it would result in every node to redesign its own particular routing table in like manner. Accordingly, the packets from nodes 1 to 2 navigate node 3

instead of node 0 and 5. Thus, node 3 can drop and control the activity between nodes 1 and 2. We expect, as node 3's one-hop neighbors, both node 2, node 5, and node 6 get the interruption alarms with 80 percent certainty from their separate IDS modules. Figs. 4a, 4b 4c demonstrate the steering tables of Hubs 2, 5, and 6 preceding the assault, after the assault and after the detachment, separately. We set a=0.2, b=0.7, c=0.8, d=0.05, If1=5, If2=7, If3=10, If4=3, If5=3, Lt=-0.0017, Ut=1 and n=5 in our analyses.

TABLE 1
Hazard assessment and Decision Making

		Node		
Approaches	**Index**	**2**	**5**	**6**
Binary	**Decision**	**Isolation**	**Isolation**	**Isolation**
DRC	H_A	0.00011	0.00000057	0.00000057
	H_C	0.00166	0.0016	0.0144
	Hazzard	-0.00154	-0.00162	-0.01439
	Decision	Isolation	Isolation	Isolation
DRCIF	$_{HA}$	0.467	0.00355	0.00355
	$_{HC}$	0.0134	0.0134	0.1
	Risk	0.4534	-0.01005	-0.096
	Decision	Isolation	No Isolation	No Isolation
	Time	304ms	0	0

We analyze binary isolation methodology, risk recognition approach with DRC, and danger identification approach with DRCIF to compute the reaction choices for nodes 0, 4, and 6. As demonstrated in Table 1, parallel confinement recommends all nodes to isolate the threatening one since it doesn't consider countermeasure hazard. With our danger discovery reaction instrument focused around our amplified D-S hypothesis, node 1 ought to be segregated just by node 0 while the first D-S hypothesis would recommend that both nodes 0 and 4 isolate node 1. In Fig. 5a, because of routing assaults, the packet conveyance proportion diminishes in Stage 2. In the wake of performing binary isolation and DRC risk location reaction in Stage 3, the packet conveyance degree even reductions more. This is on account of these two paired separation and DRC peril discovery reaction in Stage 3, the packet conveyance proportion even declines more. This is on account of these two reaction components generally annihilate the topology of system. Then again, the packet delivery ratio utilizing our DRCIF risk discovery reaction in Stage 3 is higher than those of the previous two reaction systems. In Fig. 5b, the routing assaults expand the routing cost in Stage 2. As opposed to recuperating the routing cost in Stage 3, binary isolation and DRC risk location reactions build the directing expense. DRCIF danger recognition reaction, then again, diminishes the routing expense. Contrasted and other two reaction systems, it shows that our DRCIF risk discovery reaction successfully handles the assault.

Figs. 5c and 5d demonstrate the packet and byte overhead, individually. Since the routing assaults don't change the system topology further in the given case, the packet overhead and byte overhead remain practically the same in Stage 2. In Stage 3, nonetheless, they are higher when our DRCIF risk recognition reaction system is connected. This result meet our desire, on the grounds that the quantity of hubs which detach threatening node utilizing binary isolation and DRC risk discovery reaction are more prominent than those of our DRCIF peril recognition reaction system. As indicated in Table 1, the quantity of isolated nodes for every system differs.

In Fig. 5e, as an outcome of the routing assaults, the mean dormancy increments in Stage 2. After reaction, we perceive the mean latencies in Stage 3 for three diverse reaction instruments have pretty nearly the same results. In Fig. 5f, the normal way length diminishes in Stage 2 because of the threatening activity guaranteeing a shorter way performed by node 1. After reaction, the normal way length utilizing double separation is higher than those of the other two reaction instruments in light of the fact that more nodes isolated the dangerous node focused around the way of parallel isolation. Thus, a few packets may be retransmitted by a greater number of hops than in the recent past.

VI. CONCLUSION

A uncertainty-aware response solution for mitigating MANET routing attacks is proposed. The method considered the potential harms of assaults and countermeasures. Keeping in mind, the end goal to quantify the uncertainty of both attacks and countermeasures, Dempster-Shafer theory of evidence is extended with an idea of significance components. In light of a few measurements, it is likewise researched the execution and common sense of our methodology and the investigation comes about plainly showed the adequacy and adaptability of our uncertainty aware approach.

References

1. Y. Zhang, W. Lee, and Y. Huang, \Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.
2. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wire-less Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.
3. P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, \Secu-rity in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st Interna-tional Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.
4. O. Kachirski and R. Guha, \E®ective Intrusion Detection Using Multi-ple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th An-nual Hawaii International Conference on System Sciences (HICSS'03),p. 57.1, January 2003.
5. Y. Hu, D. B. Johnson, and A. Perrig, \SEAD: Secure E±cient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of the 4th IEEE Workshop on Mobile omputing Systems and Applica-tions (WMCSA'02), pp. 3-13, June 2002.
6. Y. Hu, A. Perrig, and D. B. Johnson, \Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," Proceedings of the 8th An-nual International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, September 2002.
7. A.Perrig, R. Canetti, D. Tygar and D. Song, \The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, 5 (Summer), 2002.
8. 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.
9. 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.
10. 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.
11. 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.
12. G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.
13. 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.
14. 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.
15. K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.
16. L. Zadeh, "Review of a Mathematical Theory of Evidence," AI Magazine, vol. 5, no. 3, p. 81, 1984.
17. R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93-137, 1987.
18. 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.
19. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.
20. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
21. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
22. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.
23. 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.
24. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.
25. 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.
26. K. Fall and K. Varadhan, "The NS Manual," 2010. [20] F. Ros, "UM-OLSR Implementation (version 0.8.8) for NS2," 2007.
27. 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.
28. 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.
29. 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.
30. 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," ACM Trans. Information and System Security, vol. 10, no. 4, pp. 1-35, 2008.

31. C. Tseng, S. Wang, C. Ko, and K. Levitt, "DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for Manet," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 249-271, 2006.

32. 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.

33. N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.

34. 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, pp. 233-245, Mar./Apr. 2011.

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

36. 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.

37. 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.

38. T. Toth and C. Kruegel, "Evaluating the Impact of Automated Intrusion Response Mechanisms," Proc. 18th Ann. Computer Security Applications Conf. (ACSAC '02), pp. 9-13, 2002.

39. 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.

40. 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.

41. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in Proc. 12th Int. World Wide Web Conf., May 2003, pp. 640–651.

AUTHOR(S) PROFILE

B.Hariprasad,completed M.sc Computer Science, pursuing M.Tech, at SITE Engineering College, Andhraprdesh, India

Sri A. Narayanarao *M.Tech,(Ph.d)* Head of the Department of Computer Science, SITE Engineering College

Sri. O. Devakiran *M.Tech*, Assistant Professor, SITE Engineering College

