An Efficient Approach to Eliminate Routing Attack in Wireless Network

[1]R. Senthamil Selvan,
[1]PG Student,,
Department of Computer Applications,
Sathyabama University,
Chennai- 600 119,

[2]Mrs. C. Deepa
Asstant Professor
Faculty of Computing
Sathyabama University,
Chennai- 600 119,

***Abstract*— Wireless networks, routing attacks are intended to harm the network. Dempster - Shafer theory provide a solution for routing attacks. The critical importance of reducing attacks is with a combination of factors works on the principle of Dempster rule.The main drawback of this system is, after attack is occurred every time the intrusion detection system has to send an alert message and changes has to be made in the routing table. In order to avoid this problem, the knowledge based intelligent system is proposed. In this system, if a source node needs to send a data to the destination node, first it has to get an authorized path from the intelligent node, which is nothing but node with high energy. This system is discussed with the four routing attacks such as route salvage, sleep deprivation, colluding miss relay and collision attack.**

***Index Terms*— Wireless networks, intrusion response, dempster-shafer theory.**

I. INTRODUCTION

On a shared wireless medium predefined wireless network infrastructure, operation and maintenance of the network is responsible for communicating with each other without the presence of the components (nodes). Each node in the wireless network, communicate with other nodes with the help of vicinity [8], is equipped with a wireless transmitter and receiver. The wireless nodes that are not in the vicinity of rules to be followed, hopping sequence (routing protocol) following is a set of hop to hop communicate with each other .series of interconnected nodes that constitute a valid and is optimal . This is known as multi- hop communication.

Dynamism of Topology: Wireless network nodes randomly [9], and often occur within the mobile network. These nodes, there by significantly between nodes and routing complexity of the position of trust to influence, or to leave the network at any point of time can be involved. This focuses on the dynamics of the network topology as well as Connectivity between. The hosts are unpredictable. A node participating in the network environment is a function of management.

Lack of fixed infrastructure: In [9] the absence of a fixed infrastructure or central wireless network is a key feature. The network attributes to control eliminates the possibility of establishing a centralized authority. The reason for this lack of authority and protection of the traditional network management techniques are hardly applicable to wireless networks.

Resource constraints: By default network are limited power capacity, computational power, memory, bandwidth, etc. is a set of mobile devices. To achieve a secure and reliable communication between the nodes, the lack of these resources works more durable. Delays in security requirements (availability, the confidentiality, integrity and authentication, non- repudiation) decide whether to networks or wireless networks, wireless networks due to its inherent characteristics from the fixed network are susceptible to security attacks remain the same regardless. The lack of a central agency to provide protection inhibits the classical server-based solution .entails. There are several features of DS theory. First, the basic probability assignment function and confidence to represent both subjective and objective evidence enables. Second, it is possible to combine logic evidence together with Dempster 's rule of combination (DRC) supports . To address these limitations in the wireless network intrusion response scenario, we model the importance of DS evidence factors
(EF) in combination with the notion introduce a new Dempster 's rule .

Colluding Miss Relay Attack: Several attackers work in collusion to modify or drop routing packets to interrupt routing operation in a MANET.[2]

Route Salvage Attack: Route salvage attacks introduced by greedy internal nodes in the network. Generally in wireless networks there is no proper guarantee to each transmitted will reach the destination node.[2]

Sleep Deprivation Attack: Attacker node makes path busy by sending unnecessary message and drained off battery power.[2]

II. PROBLEM DEFINITION

A. Related Work*:*

Existing system is consist of intrusion detection system, which is used to whenever the attacker attacks the system that time generate a message and also used to sent this message to each nodes in the network. After receiving the alert message, the routing table change detector are used to identifies the changes occurred in the network and also it makes change for every nodes in the network. Finally isolated the attacker node from the network.[1]

Wireless networks are self-configuring routing protocols connected by wireless links. Absence of central management agency or a infrastructure is a key feature of the wireless network these nodes communicate by interchange of packets. Nodes not in the wireless range go with hop by hop.

Lack Of defined central authority, secure the routing becomes a challenging thus leaving Wireless Networks vulnerable to attacks, which results in decline of performance characteristics as well as raises a serious question mark about the reliability of such networks.[2]

In [3], explained particularly learning relationship between Bayesian inference and evidence theory . Strengthen the concept of a set of probability distributions in Bayesian analysis and Dempster - Shafer theory is central in some versions of both. Most of literature as regards these two principles. We considered as evidence and as such, DS structures can be represented, both of which imprecise likelihoods and priors, as hip recoverable imprecise interpretation of imprecise probabilities. Natural and simple robust combination operator of the pair -wise combinations of the elements of two sets. A particular family of DS structures imprecise delivery, Choquet capacity can represent. These are not closed under the rules of our combination, but can be done by rounding. The proposed combination operator is unique, and interesting, authentic and factual properties. We have examples of other proposed fusion rules Zadeh compare their behavior. We also show how paradoxical reasoning method appears robust framework

Personal vehicle in vehicular ad-hoc networks can help each other find resources establish reliability under highly dynamic conditions. That provides a way for such networks present a reputation management system. They demonstrate the effectiveness of data-intensive reputation management plan to present the preliminary simulation results. This scheme considers cooperativeness and accuracy of peer provided data as two aspects of trust when evolving trust relationships and managing reputations. use an epidemic data exchange protocol that incorporates reputation and agreement to ensure high reliability of data and stimulate proactive collaboration above and beyond stipulation.[4]

Cost-sensitive intrusion response has gained significant interest, due to its importance on the balance between potential damage by the intrusion and cost of the response. However one of the challenges in implementing this approach on the basis of system requirements and policy in a consistent and adaptable measurement of these cost factors are defined. In this paper, we evaluate and select for cost-sensitive intrusion response presents a host-based framework. Specifically. Set of measurements that characterize the potential costs associated with the intrusion handling process, and propose an intrusion response method with respect to the risk of potential intrusion damage [5].

The landscape of security threats and attacks are becoming more serious and continues to grow with the increasing number of weaknesses. To manage these risks, primarily to detect many security studies, focusing on improving prevention and response capacity, have been introduced in recent years. [6] .Antivirus software such as firewalls and security tools available to combat However, intrusion detection systems and intrusion prevention systems such as similar devices are still the most popular methods. Identification, prevention and response system aimed at enhancing the efficiency and reliability of the intrusion detection are hundreds of published works. Intrusion detection system, advanced technology, whilst the available areas to explore, especially with regard to the process of selecting the appropriate response, there still are. In this way, active, reactive and passive responses as feedback while supporting a variety of options to select the most appropriate response in different contexts enables security analysts . In view of this, little people, as opposed to a systematic approach that identifies key events needs first .will help to focus security analysts. To achieve this objective, this study combines extensive literature review, identified by model and strategy which proposed a novel framework. Set up a model to estimate the level of risk events Risk Index Model (RIM) is named . Passive responses to events with low impact while with different levels of risk , response strategy model (RSM) dynamic , proactive responses to minimize their impact is being mapped with serious incidents , the response of various map of types of events . The combination of these models provides a seamless way to automatically map the event , but it should be evaluated in terms of its effectiveness and performance . To display the results, an evaluation study has four stages, these stages , such weaknesses Scoring System and snort , as an examination of the impact of different strategies with industry standards a feasibility study of the studies were rated rim and ranking process , and response strategy model (RSM) is a test of the effectiveness and performance . Used in this study was to examine the effectiveness ; promising results have been gathered , a proof-of-concept study to prioritize security events module (SIPM) online assessment through simulation mode with live traffic network was conducted to demonstrate the structure practicality. Through the results gathered, this study has demonstrated that the prioritization process can feasibly be used to facilitate the response selection process in Intrusion Response Systems. The main contribution of this study is to have proposed, designed, evaluated and simulated a framework to support the incident prioritization process for Intrusion Response Systems.

III. PROPOSED MODEL

Proposed system is used to eliminate routing attacks by using DSR routing protocol and Dempster Shafer theory. Intelligent node which monitors the network and find intruders after that gives an alert. It is designed with loop free routing. Intermediate nodes don’t contain the routing information. The main task of this **intelligent node** is to distribute the key using SHA to entire nodes in the network. Thus the nodes in the network are trained. Whenever the intelligent node sends key request to node, the already trained nodes reply to the intelligent node queries while the attacker node couldn’t reply to the intelligent node. Because the attacker does not aware about the key.

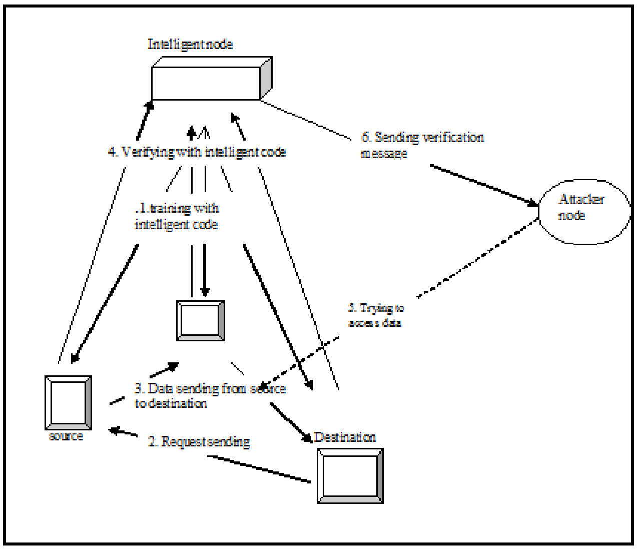

Intelligent node
4. Verifying with intelligent code
6. Sending verification message
Attacker node
.1.training with intelligent code
5. Trying to access data
3. Data sending from source to destination
source
2. Request sending
Destination

Fig 1. Proposed System Architecture

Proposed model deals with two algorithms whereas use for finding shortest path and key distribution.

A. *Dijkstra's Algorithm*

In [7] Dijkstra's algorithm that solves the single-source shortest path problem for a graph with non-negative edge path costs, producing a shortest path tree. This algorithm is often used in routing and as a subroutine in other graph algorithms.

```
function Dijkstra(Graph, source):
for each vertex v in Graph:
dist[v]  := infinity
previous[v]  := undefined ;
end for
dist[source]  := 0 ;
Q := the set of all nodes in Graph ;
while Q is not empty:
u := vertex in Q with smallest distance in
dist[] ;
remove u from Q ;
if dist[u] = infinity:
break ;
end if
for each neighbor v of u
alt := dist[u] + dist_between(u, v) ;
if alt < dist[v]:
dist[v]  := alt ;
previous[v]  := u ;
decrease-key v in Q;
end if
```

```
end while
return dist;
end function
```

B. Secure Hashing Algorithm*:*

SHA1 stands for "Secure Hashing Algorithm". It is use to distribute the key for each node for authentication process.

SHA1 Algorithm Description

Padding

1)Pad the message with a single one followed by zeroes until the final block has 448 bits.

2)Append the size of the original message as an unsigned 64bit integer.

Initialize the 5 hash blocks (h0,h1,h2,h3,h4) to the specific constants defined in the SHA1
standard.

4) Hash (for each 512bit
Block)

5) Allocate an 80 word array for the message schedule

6) Set the first 16 words to be the 512bit
block split into 16 words.

7) The rest of the words are generated using the following
algorithm

8) word[i3]
XOR word[i8]
XOR word[i14]
XOR word[i16]
then
rotated 1 bit to the left.

9) Loop 80 times doing the following. (Shown in Image1)

10) Calculate SHAfunction() and the constant K (these are based on the
current round number.

11) e=d

12) d=c

13) c=b (rotated left 30)

14) b=a

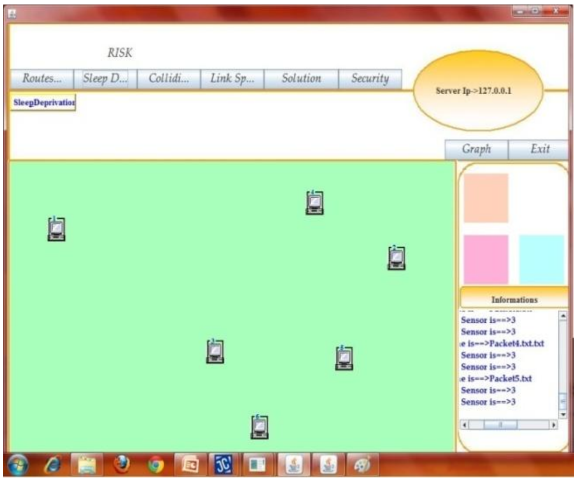
15) a = a (rotated left 5) + SHAfunction() + e + k + word[i]

16) Add a,b,c,d and e to the hash output.

17) Output the concatenation (h0,h1,h2,h3,h4) which is the message digest. of a RGB color TIFF file should be at least 400 dpi.

IV. RESULTS AND DISCUSSION

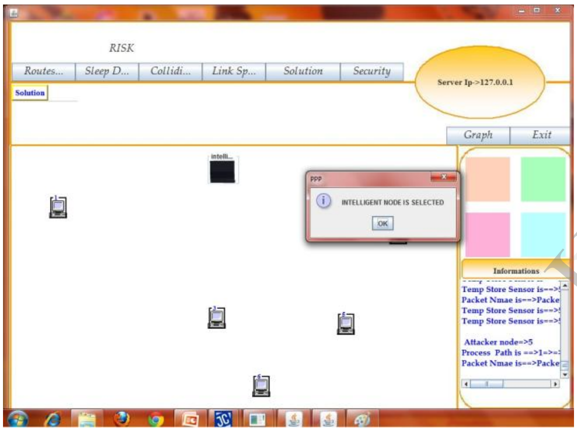
As of my proposed model create some nodes for assumption create six nodes in particular area. After node creation done energy calculation(battery power) will begins in which highest power will be consider as an intelligent node and this node will training the other nodes by giving key value. By using these key value intelligent node will identify whether it is an attacker node or node. Since it is wireless network every node battery power will drained off for each transaction so based on time limits energy will be calculated and again reassign some other node as intelligent node.



Sensor is==>3
Sensor is==>3
e is==>Packet4.txt.txt
Sensor is==>3
Sensor is==>3
e is==>Packet5.txt
Sensor is==>3
Sensor is==>3

Fig 2. Network Creation

In Fig 2 node are created based on our assumption. In the same screen we can see the information about each and every node and location of each node will be select by user with the help of pointing device.



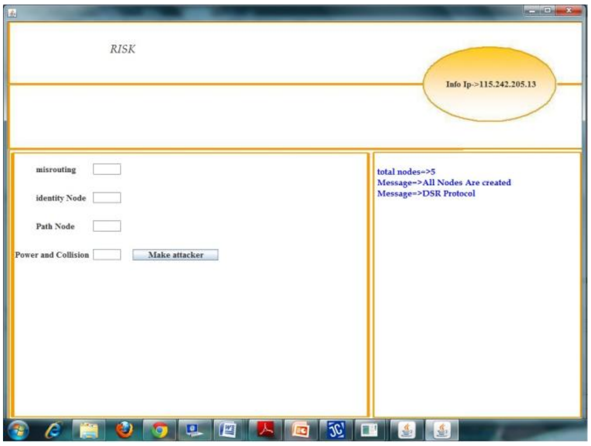
INTELLIGENT NODE IS SELECTED

Temp Store Sensor is==>5
Packet Nmae is==>Packe
Temp Store Sensor is==>5
Temp Store Sensor is==>5

Attacker node=>5
Process Path is ==>1=>=
Packet Nmae is==>Packe

Fig 3. Intelligent Node

In Fig 3 intelligent node is selected based on battery power of each node. This node will give training for each node by assigning some key value for each node.

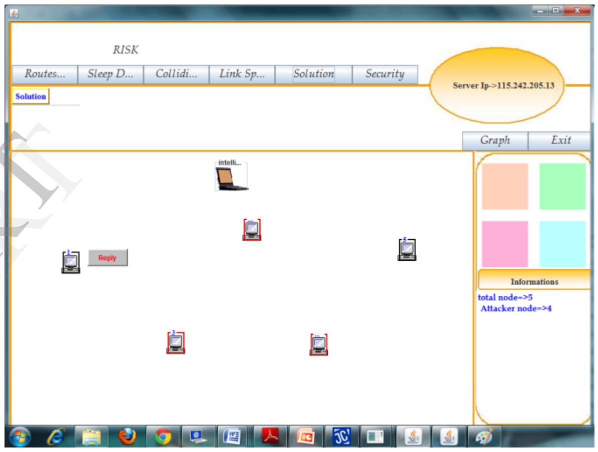


misrouting □
identity Node □
Path Node □
Power and Collision □

total nodes=>5
Message=>All Nodes Are created
Message=>DSR Protocol

Fig 4. Creating Attack

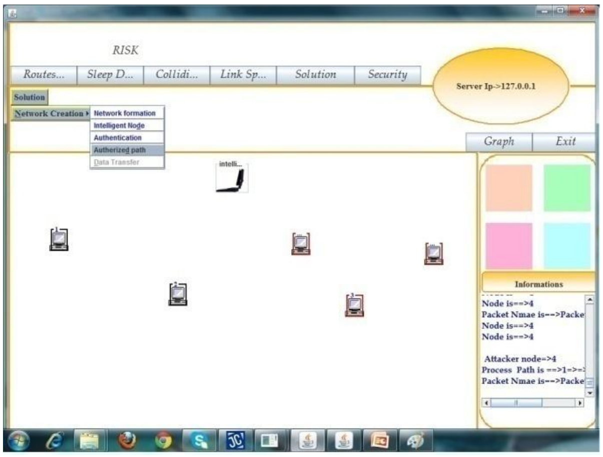
In Fig 4 shows screen for creating attack in this screen user can create some node as attacker node. In this paper we discuss with four attacks.



total node=>5
Attacker node=>4

Fig 5. Authentication (Key)

In Fig 5 shows authentication process whereas intelligent node will verify each node by asking key value.

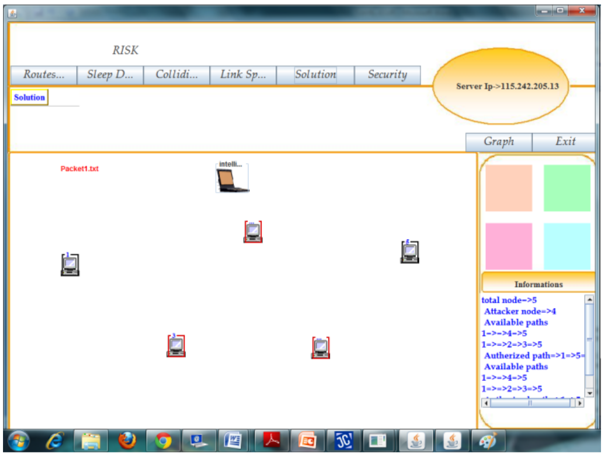


Node is==>4
Packet Nmae is==>Packe
Node is==>4
Node is==>4

Attacker node=>4
Process Path is ==>1=>=
Packet Nmae is==>Packe

Fig 6. Authorized Path

In Fig 6 shows authorized path based on the authentication process. Intelligent node will gave a secure path for source node to make data transfer



```
total node-->5
 Attacker node=>4
 Available paths
1->->4->5
1=>=>2=>3=>5
 Autherized path=>1=>5=
 Available paths
1->->4->5
1=>=>2=>3=>5
```

Fig 7. Data Transfer

In Fig 7 shows data transfer process in secure path.

V. CONCLUSION

This paper proposes a new secure data transmission method in the Wireless Network with the help of intelligent node. Nodes are trained when the network is deployed. If a source node needs to send the packet to the destination node, it has to request the authorized path to the intelligent node. Then the intelligent node sends key request to all the nodes in the network. After receiving the key request, the node sends key reply to the intelligent request as nodes are already trained. With the help of this we can transmit the data's throughout the Wireless Network without any attacks or leakage of data

REFERENCES

1. Ziming Zhao, Gail-Joon Ahn, MARCH/APRIL 2012" Risk-Aware Mitigation for MANET Routing Attacks" ieee transactions on dependable and secure computing, vol. 9, no. 2,pp.250-260.
2. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Nato," a survey of routing attacks in mobile ad hoc networks" ieee wireless communications • october 2007,pp.86-91.
3. Stefan Arnborg ,Kungl Tekniska H¨ogskolan, Stockholm, "Robust Bayesianism: Imprecise and Paradoxical Reasoning".
4. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks" computers, ieee transactions on Vol 59 no 5.pp.707-719
5. S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks".
6. L C. Mu, X. Li, H. Huang, and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory".
7. Alispahic, N. Elma, A. lvana, K. Elma, L. Nosovic, "Dijkstra's shortest path algorithm serial and parallel execution performance", MIPRO, 2012 Proceedings of the 35th International Convention,pp.1811 - 1815.
8. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", journal of computing, volume 3, issue 1,,pp.41 - 48.
9. Dr Venkata Surya Narayana T, *M. Ambica, P. Datta Dev, Y.Bala TripuraSundari,*" A Study On Black Whole Attacks In Mobile Ad Hoc Networks" ieee transactions on dependable and secure computing, vol. 9, no. 2,PP.793-796.