Detection and Resolving of Black Hole Attack in Wireless Mesh Network using Colored Petrinet Model

Ms. Deepa S Angadi
Asst.prof,
Dept. of Computer Science & Engineering
S.G.Balekudri Institute of Techology, Belgaum

Prof. P. S. Khangoudar
Asst.prof,
Dept. of Computer Science & Engineering
Gogte Institute of Technology,Belgaum

Abstract:- **Security is always a major concern and a topic of hot discussion to users of Wireless Mesh Networks (WMNs). The open architecture of WMNs makes it very easy for malicious attackers to exploit the loopholes in the routing protocol. Cooperative Black-hole attack is a type of denial-of-service attack that sabotages the routing functions of the network layer in WMNs. This project is concentrating on improving the security of one of the popular routing protocols among WMNs, Ad-hoc on demand distance vector (AODV) routing protocol and present probable solution to this attack using Merkle hash tree. There exist another efficient technique for modeling and resolving of the black hole attack in WMN based on colored Petri net (CPN).CPN provides a graphical representation of the protocol, and there exists a large variety of simulation tools and mathematical methods for analysis. To the best of our knowledge, it is the first time that colored Petri net is applied to handle the security issue in Wireless Mesh Networks.**

Key words: Colored petrinet, wmn ,black hole.

1. INTRODUCTION

Wireless mesh network (WMN) has emerged as a key technology for next-generation wireless networking. Because of their advantages over other wireless networks, WMN is undergoing rapid progress and inspiring numerous applications. A WMN is dynamically self- organized and self-configured; the nodes in the network automatically establish and maintain mesh connectivity among them. As a new wireless mobile network, WMN is vulnerable to security attacks, such as eavesdropping, forgery, denial of service attacks. Black hole attack [1] is a serious security problem to be solved. The black hole attack in WMN is depicted in Figure 1. Without loss of generality, suppose there are many paths from source node *S* to the destination node *D* and *B* is the malicious node. Once *B* received the RREQ, it will send the RREP to *S* and announces that *B* is in the shortest path from *S* to *D*. Then all the packets will be sent to the malicious node *B*. In this way, the black hole attack happens.

This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.This kind of attack results in many detecting methods fail and causes more immense harm to networks.

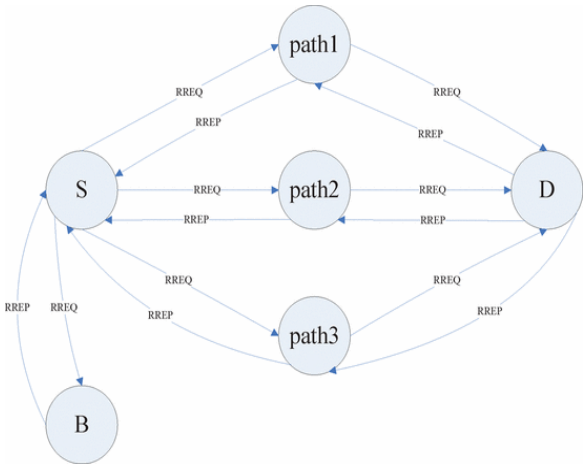


Figure 1. The black hole attack in WMN

We expect a secured WMN to have accomplished objectives such as confidentiality, integrity, availability, authenticity, non-repudiation, authorization and anonymity. In this section, some of the most critical threats and attacks present at network layer are discussed.

A. Black-hole attack:

In this attack, the malicious node always replies positively to a route request from a source node although it may not have a valid route to the destination and will always be the first to reply to the route request message. Therefore, all the traffic from the source node will be directed toward the malicious node, which may drop all the packets, resulting in DoS [18].

B. Wormhole attack:

To launch this attack, an attacker connects two distant points in the network using a direct low latency communication link called the wormhole link. Once the wormhole-link is established, the attacker captures wireless transmission on one end, sends then through the wormhole link, and replays them at the other end [16]. Then the attacker starts dropping packets and cause network disruption. The attacker can also spy on the packets going through, use the information gained to launch new attacks, and thus compromise the security of the network.

C. Sink-hole attack:

In this attack, a malicious node can be made very attractive through the use of powerful transmitters and high-gain antennas to the surrounding nodes with respect to the routing algorithm [17].

D. Sybil Attack:
This attack is defined as a "malicious device illegitimately taking on multiple identities" [19]. This attack abuses the path diversity in the network used to increase the available bandwidth and reliability. The malicious node creates multiple identities in the network. The legitimate nodes, assuming these identities to be distinct network nodes, will add these identities in the list of distinct paths available to a particular destination thus including the malicious node on path of a data, which can affect packet transfer as well as drop them. But, Even if the malicious node does not launch any attack, the advantage of path diversity is diminished, resulting in degraded performance [17]. But prevention of black hole attack using merkle tree is not suitable when there are more number of black hole nodes exists.

2. ABOUT THE EXSITING TECHNIQUES

In recent years, researchers propose different solutions for black hole problem. Po-chun Tsou et al. propose a DSR-based secure routing protocol [2], named BDSR. The BDSR detects and avoids the black hole attack based on merging proactive and reactive defense architecture by using the virtual and non-existent destination address to bait the malicious node to reply RREP. William Kozma Jr et al. propose a novel misbehavior identification scheme called REAct that provides resource-efficient accountability for node misbehavior [3]. REAct identifies misbehaving nodes based on a series of random audits triggered upon a performance drop. They show that a source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioral proofs provided by nodes. Proofs are constructed using Bloom filters which are storage-efficient membership structures, thus significantly reducing the communication overhead for misbehavior detection.

The authors in [4] [5] present an algorithm for preventing the cooperative black hole attacks. They address the problem of coordinated attack by multiple black holes acting in group, and then present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Vishnu K et al propose to use the concept of Backbone network [6]. Backbone nodes are a group of nodes which are powerful in terms of battery and range. Backbone network is formed with these nodes which are permitted to allocate restricted 1P addresses (RIP) to newly arrived nodes. The authors address the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black and gray or hole attacks. The technique is capable of finding chain of cooperating malicious node which drop a significant fraction of packets.

Most proposed solutions for the black hole attack in WMNs have not been verified with formal methods. Meanwhile, the verification of cryptographic protocols has gained a lot of interest in the research community. Currently, there are three kinds of formal methods used for the analysis of cryptographic protocol. The first one is based on logic. Such as BAN logic [7], GNY logic [8], and MAo logic [9]. This kind of method builds a logic model for the protocol, and reason in terms of logical propositions. The second one is based on algebra, e.g., CSP algebra [10]. These methods involve modeling the protocol as algebraic system, and reason in terms of the algebraic properties of the model. The last one is based on state machines. They include Petri-net and NRL Analyzer [11]. This kind of method involves modeling the protocol in terms of a general modeling tool that enumerates the state space, and then analyzing the model in terms of state invariants.

The above mentioned formal methods mainly have the following characteristics [12]: 1) several formal methods may use computerized tools for analysis. For example, most of the state machine based methods can use an automated tool to construct and analyze the state space. on the other hand, logic based methods are hard to automate since they involve non-trivial proofs; 2) Some methods, especially those based on logic and algebra, can be used to formally prove that a security property is satisfied by a given cryptographic protocol. Such methods state the properties of intruder actions and reason in terms of deduction rules. other methods, e.g., most of those based on state machines, are geared toward determining the existence of certain flaws rather than guaranteeing that flaws do not exist in a given cryptographic protocol. Such methods require explicitly stating the possible intruder attacks. Thus they will be helpless in detecting attacks not included in the model.

3. PROBLEM DEFINITION

Petri Nets is a formal and graphical appealing language which is appropriate for modelling systems with concurrency. Petri Nets has been under development since the beginning of the 60'ies, where Carl Adam Petri defined the language. It was the first time a general theory for discrete parallel systems was formulated. The language is a generalization of automata theory such that the concept of concurrently occurring events can be expressed. Petri Nets can be used to model a wide range of various systems.

Colored Petri Nets (CPNs) are an extension of ordinary Petri Nets. CPNs provide a modeling framework suitable for simulating distributed and concurrent processes with both synchronous and asynchronous communication. They are useful in modeling both nondeterministic and stochastic processes as well. CPNs extend the vocabulary of ordinary Petri Nets and add features that make them suitable for modeling large systems. CPNs combine the strengths of ordinary Petri Nets with the strengths of a high-level programming language called CPN ML which is based on the functional language SML (Ullman 1998). Petri Nets provide the primitives for process interaction, while the programming language provides the primitives for the definition of data types and the manipulations of data

values.
CPN Tools has an intuitive graphical user interface that is useful for editing, simulating, and analyzing Colored Petri nets. The tool features incremental syntax checking and code generation, which take place while a net is being constructed. CPNs provide a unified approach for analysis of both functional/logical properties as well as performance properties through their support for both timed and untimed activities within a single formalism. Thus one does not have to create two separate models to carry out such analyses. Furthermore, unlike many discrete event simulation systems, CPNs provide a set of state space methods for verification of system properties.
The state space approach complements analysis that can be performed based on pure simulation. CPNs support a mechanism of modules for construction of large system models in a hierarchical manner. The hierarchy and module concept of CPNs permit different levels of abstraction that are inherent in most complex systems. The graphical representation makes it easy to see the basic structure of a complex CPN model and understand the interaction of individual sub-components.

4. CHALLENGES OF THE PROPOSED SYSTEM

To cope with the complexity of modern concurrent systems, it is crucial to provide methods that enable debugging and testing of central parts of the system designs prior to implementation and deployment. One way to approach the challenge of developing concurrent systems is to build an executable model of the system. Constructing a model and simulating it usually lead to significant new insights into the design and operation of the system considered and often results in a simpler and more streamlined design. Furthermore, constructing an executable model usually leads to a more complete specification of the design and makes it possible to make a systematic investigation of scenarios which can significantly decrease the number of design errors. The construction of a model of the system design typically means that more effort is spent in early phases of system development, i.e., requirements engineering, design, and specification. This additional investment is, in most cases, justified by the additional insight into the properties of the system that can be gained prior to implementation. Furthermore, many design problems and errors can be discovered and resolved in the requirements and design phase rather than in the implementation, test, and deployment phases. Finally, models are, in most cases, simpler and more complete than traditional design a document which means that the construction and exploration of the model has resulted in a more solid foundation for doing the implementation. This may in turn shorten the implementation and test phases significantly and decrease the number of flaws in the final system.
The development of CP-nets has been driven by the desire to develop an industrial-strength modelling language— at the same time theoretically well-founded and versatile enough to be used in practice for systems of the size and complexity found in typical industrial projects. CP-nets are, however, not a modelling language designed to replace other modelling languages (such as UML). In our view it should be used as a supplement to existing modelling languages and methodologies and can be used together with these or even integrated into them. High-level Petri Nets is an ISO/IEC standard and the CPN modelling language and supporting computer tools conform to this standard. The practical application of CP-nets typically relies on a combination of interactive and automatic simulation, visualization, state space analysis, and performance analysis. These activities in conjunction result in a *validation* of the system under consideration in the sense that it has been justified that the system has the desired properties and a high degree of confidence and understanding of the system has been obtained. CPN models can be used to validate both the functional/logical correctness and the performance of a system. This saves a lot of time, because we do not need to construct two totally independent models of the system. Instead we can use a single model or (more often) two models that are very closely related to each other. There exist a number of modelling languages that are in widespread use for performance analysis of systems, e.g., queuing theory. However, most of these modelling languages cannot be used for modelling and validation of the logical properties of systems. Some of these are also unable to cope with performance analysis of systems which have irregular behaviour.

5. LITERATURE SURVEY

In the best of our knowledge, till now, there is no IDS exclusively designed for WMN. To date the existing IDS designed for multi-hop wireless networks are mostly based on the characteristics of MANET such as follows:
• Temporary network which has no support of routers and gateways; instead the nodes also perform the routing functionality.
• Application specific which is used mostly for emergency situations such as natural disasters or battle fields.
• Served by mobile nodes which posses power and bandwidth constraint.
• The traffic pattern is from users to users. The existing cooperative and hierarchical IDS are MANET based. The entire intrusions detection and monitoring mechanisms are implemented in MANET nodes. These IDS ensures the cooperation amongst the MANET nodes to collectively monitor the intrusions and in case of intrusion found, then inform each other, or the cluster head which is responsible for intrusion detection of all its child nodes. Furthermore there is no question of involvement of the routers and gateways in MANET IDS. As compared to MANET, the WMN has significant different network characteristics, that is why, proposing or investigating any IDS, there is a need to keep under consideration the characteristics of WMN, as well as the following important facts:
• As a large scale broadband network, WMN consists of fixed backbone mesh routers and gateways infrastructure, which is not power constraint.

• Majority of mesh nodes are static which have no power limitations; however there is also support for mobile nodes in ad-hoc and infrastructure mode.
• WMN is an integrated technology, which can enable integration amongst other wireless networks such as IEEE 802.11 WLANs, IEEE 802.16 WMANs.
• In WMN, most of the traffic is from gateway toward the nodes through static multi-hop of access points. Keeping in view these differences, there is a need of such IDS systems which are specially designed and proposed exclusively for WMN environment. The IDS for WMN must consider its two levels i.e., end user mesh nodes and mesh routers. Intrusions and security attacks may be possible on both lower level and middle level. The utmost need is to propose an IDS that is capable to handle the intrusions at lower and middle levels, thus we can prevent the serious disruption at the top level.

TABLE I. COMPARISON OF ATTACKS AT NETWORK LAYER

Attacks	Type of Attacker	Type of Attack	Required Knowledge	Cost	Detectability
Black-hole	Insider	DoS	Low	Low	High
Wormhole	Insider & Outsider	Modify &Dos & Replay	High	High	Low
Sink-hole	Insider	Modify & DoS	Medium	Medium	Low
Sybil	Insider	Masquerade & DoS	Low	Medium	Low

As we see in the table, a black-hole attack will be favored by most attackers because any attacker whose intentions are to bring down the whole network communication at a low cost with least amount of information about the network can carry out this attack. The detect ability is surely higher than other attacks and that is why a more complex form of Black-hole attack called Cooperative Black-hole attack which is hard to detect, is being carried out by attackers. The next section takes a look in to this form of Black-hole attack.
Petri net diagrams are a recognized form of modeling real time systems and have been included in the list of UML techniques for modeling the dynamic aspects of object oriented systems. A Petri net diagram explains how workflow techniques can be used for developing models for larger independent systems. These chunks or independent systems which are part of the large systems are expressed through the use of work lets. This can then be used as the basis of modeling systems where timeliness is of importance. However, this requires extending workflow ideas to incorporate flexibility, handling of exceptions and adaptability. Extensions of the Petri net diagrams are then proposed for expressing the models obtained from such workflow techniques.

6.SIGNIFICANCE OF THE PROPOSED SYSTEM

Node File Creation
Node File
1.(2,1)
2.(5,4
3.(14,7)
4.(25,5)
5.(33,6)
6.(40,7)
7.(45,29)
8.(37,18)
9.(29,16)
10.(37,23)
11.(31,22)
12.(27,22)
13.(23,18)
14.(14,14)
15.(21,24)
16.(12,24)
17.(3,27)
18.(14,31)
19.(4,40)
20.(12,46)
21.(7,47)
22.(30,35)-gateway
23.(33,47)
24.(3,15)
25.(30,44)

Nodes are been plotted with neighboring nodes using fix topology.Neighbour table is generated as above to find the neighboring nodes. Communication range is fixed where in it detects the neighboring nodes of each node using that coverage range.

Received signal strength indicator (**RSSI**) is a measurement of the power present in a received radio signal.[1] Received signal strength based fingerprinting approaches have been widely exploited for localization. The received signal strength (RSS) plays a very crucial role in determining the nature and characteristics of location fingerprints stored in a radio-map. The received signal strength is a function of distance between the transmitter and receiving device, which varies due to various in-path interferences.
A detailed analysis of factors a acting the received signal for indoor localization. The paper discusses the fact of factors such as spatial, temporal, environmental, hardware and human presence on the received signal strength through extensive measurements in a typical IEEE 802.11b network. It also presents the statistical analysis of the measured data that defines the reliability of RSS-based location fingerprints for indoor localization.

7. SYSTEM DESIGN

Computer network is usually defined as collection of couples interconnected for gathering, processing & distributing information. Computer is used as broad term here to include devices such as work station, servers,

routers, modem, WMN etc. These computers are connected by communication links such as copper wire, optical fibers, microwaves/satellite or radio links.

System Modelling

To model a system some simplifying assumption are often required. It is important to note that too many assumptions would simplify the modelling but may lead to an inaccurate representation of the system.

Simulation is widely used in system modelling, simulation usually requires less abstraction in the model when the system is rather large & complex. A straight forward mathematical formulation may not be feasible. In this case the simulation approach is usually preferred simulation is the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of system and/or evaluating various strategies for the operation of the system.

Topology
Area of the nodes
Number of nodes
Communication Range
Bandwidth
Energy assignment
R×T Energy
Packet Transmission Rate

Initially topology is assumed and x , y coordinated of nodes are stored in data file , from data file the coordinates are read and stored in matrix from , each node is assigned the receiver signal strength (RSS), depending on distance and the neighbors of each node are found and listed as neighbors table.

8. IMPLEMENTATION

Node creation

Initially topology is assumed and x , y coordinated of nodes are stored in data file , from data file the coordinates are read and stored in matrix from , each node is assigned the receiver signal strength (RSS), depending on distance and the neighbors of each node are found and listed as neighbors table.

- ***Node plotting on GUI***

Figure

plot(x-coordinate, y-cordinate,'marker-shape','MarkerSize',20,'Color','r');

- ***Neighbor Finding***

```
Covrg=12;          %Network Coverage
xl=wnode(i).xd-covrg;    %xlower
xh=wnode(i).xd+covrg;    %xhigh
yl=wnode(i).yd-covrg;    %ylow
yh=wnode(i).yd+covrg;    %yhigh
```

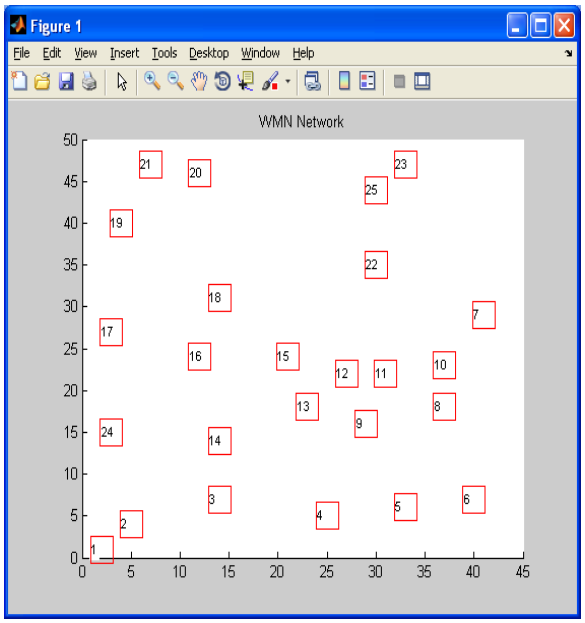
nodes within coverage area (xl yl xh yh) are considered as neighbors

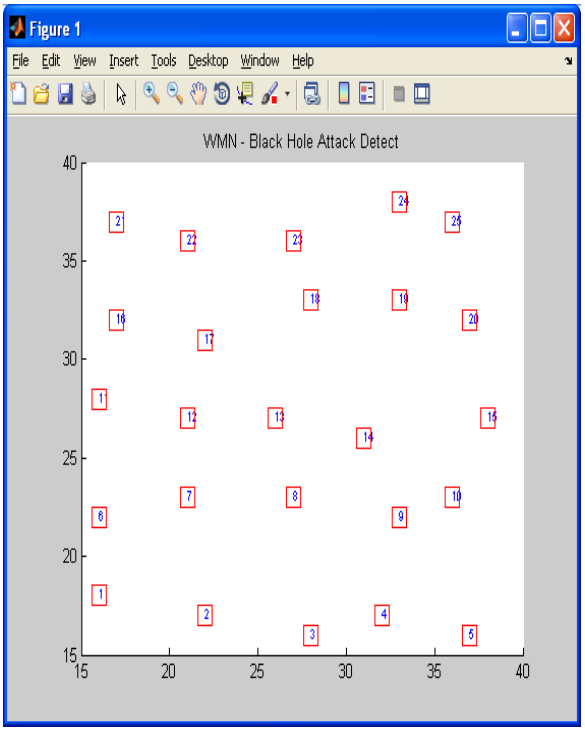
```
if (wnode(k).xd>=xl && wnode(k).xd<=xh) && (wnode(k).yd>=yl && wnode(k).yd<=yh)
        neighbours(i,nn)=k;
```

- ***On-demand route discovery***

On-demand routing protocols construct a path to a given destination only when it is required. They do not maintain topological information about the whole network, and thus there is no periodic exchange of routing information. Since the focus of our study is on the route discovery part of the protocol, we present a brief overview of the route discovery process in AODV in the remainder of this section. When a source node **S** needs a route to some destination **D**, it broadcasts a RREQ packet to its immediate neighbors'. Each neighboring node rebroadcasts the received RREQ packet only once if it has no valid route to the destination. Each intermediate node that forwards the RREQ packet creates a reverse route pointing towards the source node **S**. When the intended destination node **D** or an intermediate node with a valid route to the destination receives the RREQ packet, it replies by sending a route reply (RREP) packet. The RREP packet is unicast towards the source node **S** along the reverse path set-up by the forwarded RREQ packet. Each intermediate node that participates in forwarding the RREP packet creates a forward route pointing towards the destination **D**. The state created in each intermediate node along the path from **S** to **D** is a hop-by-hop state in which each node remembers only the next hop to destination nodes and not the entire route, as in DSR.

9. SNAPSHOTS





Command Window Output

Number of Nodes 25
Finding Neighbour nodes for each node
.....

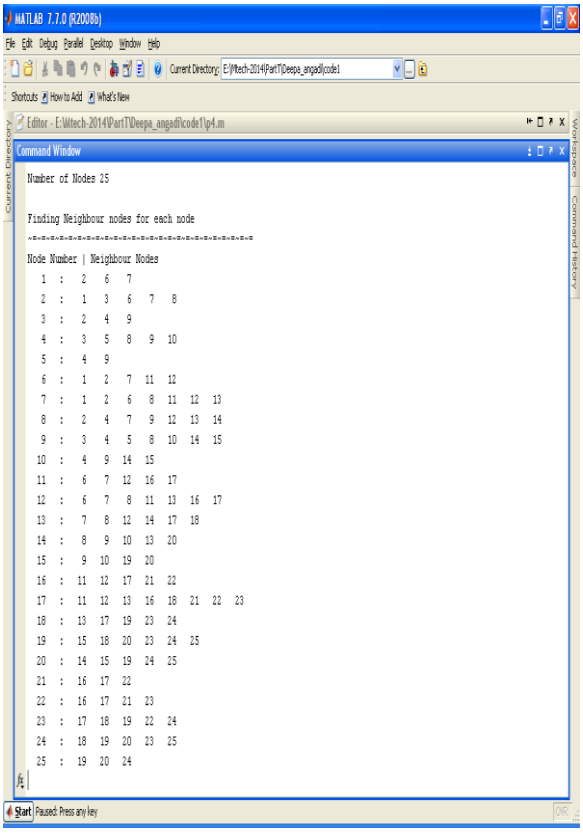
Node | Neighbours

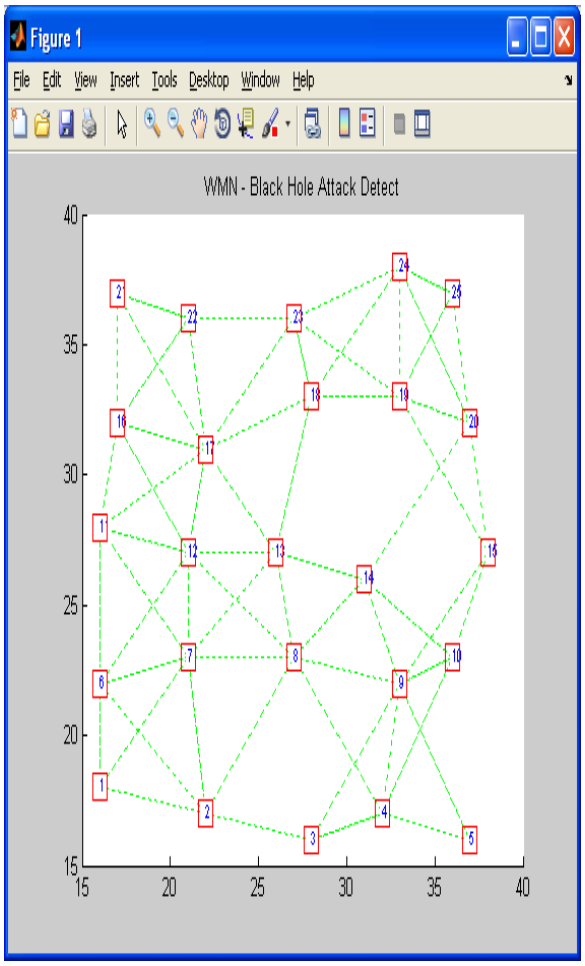
---

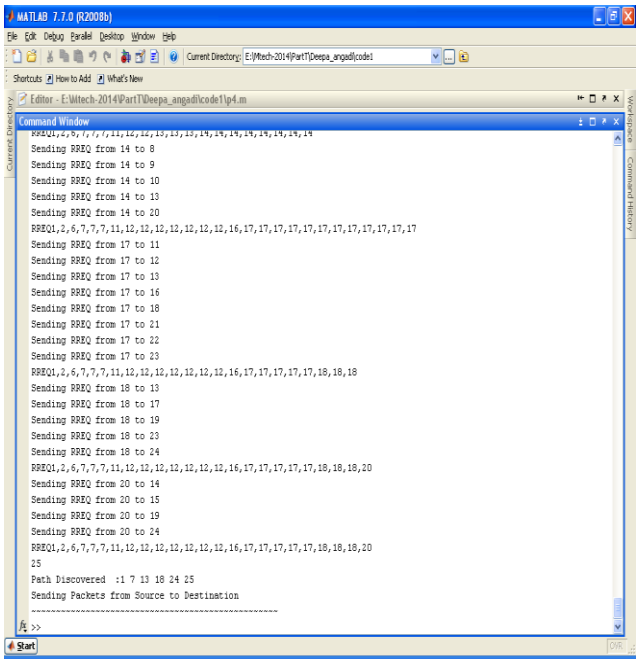
1 | 2 3
2 | 1 3 14 24
3 | 1 2 4 13 14 24
4 | 3 5 9 14
5 | 4 6 8 9 13
6 | 5 8 9
7 | 8 10 11 22
8 | 5 6 7 9 10 11 12
9 | 4 5 6 8 10 11 12 13
10 | 7 8 9 11 12 22
11 | 7 8 9 10 12 13 15
12 | 8 9 10 11 13 15
13 | 3 5 9 11 12 14 15 16
14 | 2 3 4 13 15 16 24
15 | 9 11 12 13 14 16 18 22
16 | 13 14 15 17 18 24
17 | 16 18 24
18 | 15 16 17 19

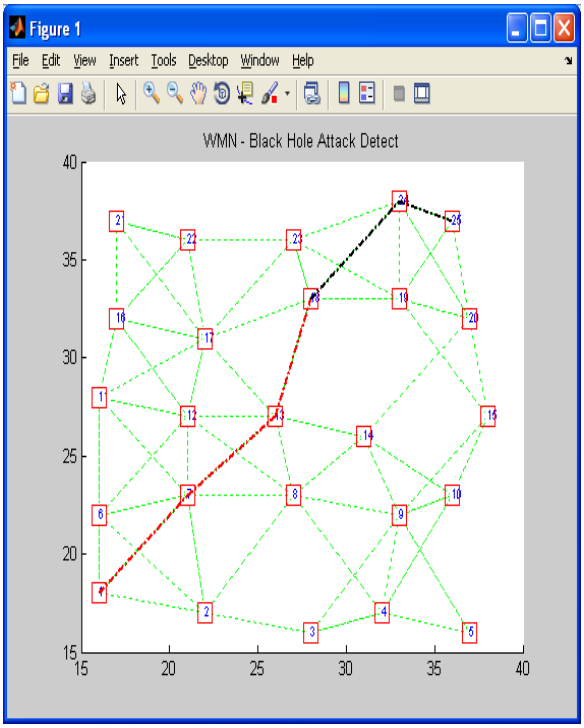
19 | 18 20 21

20 | 19 21
21 | 19 20
22 | 7 10 15 23 25
23 | 22 25
24 | 2 3 14 16 17
25 | 22 23









10. CONCLUSION

Here proposed method that uses colored Petri nets (CPN) to model and verifies the HWMP routing protocol in WMN. The CPN model of HWMP(Hybrid Wireless Mesh Protocol) can effectively simulate the process of on-demand routing part of the HWMP. The result of the state space methods and CPN Tool Simulation can successfully detect whether or not black hole attacks exist in this model. In the case black hole attacks exist,proposes a security routing algorithm based on the mechanism of public encryption. The simulation result shows that the security routing algorithm can effectively prevent the impact of the black hole attack

REFERENCES

[1] H. Deng, W. Li, and D.P. Agrawal, Routing Security in Ad HocNetworks, IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, 40(10), pp.70-75 (2002).

[2] P.C. Tsou , J.M. Chang, Y.H. Lin, H.C. Chao, and J.L. Chen, Developing a BDSR Scheme to Avoid Black Hole Attack based on Proactive and Reactive Architecture in MANETs, Advaced Communication Technology, pp.755-760 (2011).

[3] W. Kozma, and L. Lazos, REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits, Proceedings of the Second ACM Conference on Wireless Network Security, pp.103-110 (2009).

[4] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Proceedings of International Conference on Wireless Networks (2003).

[5] H. Weerasinghe and H. Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation, Proceedings of the IEEE International Conference on Coommunication (2007).

[6] V.K and A.J PAUL, Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks, International Journal of Computer Applications, 1(22),pp.38-42 (2010).

[7] M. Burrows, M . Abadi, and R. Needham, A Logic of Authentication, ACM Transactions on Computer Systems, 8(1),pp. 18-36 (1990).

[8] L. Gong, R. Needham, and R. Yahalom, Reasoning about Belief in Cryptographic Protocols, Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp.234-248 (1990).
[9] W. Mao and C. Boyd, Towards the Formal Analysis of Security Protocols, Proceedings of the Computer Security Foundations Workshop V1, IEEE Computer Society Press, pp. 147-158 (1993).
[10] P. Ryan and S. Schneider, The Modelling and Analysis of Security Protocols: the CSP Approach, Addision-Wesley, 2001.
[11] C. Meadows, The NRL Protocol Analyzer: An Overview, Journal of Logic Programming, 26(2),pp. 113-131 (1996.
[12] I. AI-Azzoni, D.G. Down, and R. Khedri, Modeling and Verification of Cryptographic Protocols Using Coloured Petri Nets And Design/CPN, Nordic Journal of Computing, 12(3), pp.201-228 (2005).
[13] T. Murata, Petri Nets: Properties, Analysis, and Applications, Proceedings of IEEE, 77(4), pp.541-580 (1985).
[14] K. Jensen, Coloured Petri Nets: Basic Concepts Analysis Methods and Practical Use, springer.verlag 1. (1997).
[15] L. J. Munoz, J. Forne, O. Esparaza, M. Soriano, "Certificate revocation system implementation based on the Merkle hash tree," Int. J. of Info. Sec. Heidelberg, vol. 2, iss. 2, pp. 110-124, January 2004.
[16] F. Nait-Abdesselam, B. Bensaou, T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad-hoc networks," IEEE Comm. Mag Canada, vol. 4, iss. 64, pp. 127-133, April 2008.
[17] V. Zhang, J. Zheng, H. Hu, Security in wireless mesh networks. Florida, USA: Auerbach Publications, 200