Invasion Discovery and Prevention Technique for Vampire Attack

by

Mogili Anitha

A research study submitted in partial fulfillment of the requirements for the degree of Master of Engineering in Information and Communication Technology

Examination Committee: Dr. Teerapat Sanguankotchakorn (Chairperson)
Dr. Attaphongse Taparugssanagorn
Dr. Poompat Saengudomlert

Nationality: Indian
Previous Degree: Bachelor of Technology in
Electronics and Communication Engineering
Jawaharlal Nehru Technological University
Hyderabad, Telangana, India

Scholarship Donor: AIT Fellowship

Asian Institute of Technology
School of Engineering and Technology
Thailand
May 2019

ACKNOWLEDGEMENT

I would like to express my profound sincerity towards Dr. Teerapat Sanguankotchakorn, my advisor for his precious guidance and constant inspiration and feeling of uplifting and the committee member, Dr. Attaphongse Taparugssanagorn for his priceless comments and recommendations for the successful completion of this special study.

I will be thankful to all members of Telecommunications department including faculties, senior students and staff, who were very helpful and nurtured me in accomplishment of this special study. I also feel grateful to be a part of the institute which helped me through its excellent facilities, various equipment and great environment to study.

I would also like to thank with my deepest gratitude to my parents and family members for their love, support and valuable encouragement ad my friends for supporting me during my stay in AIT.

M. Anitha
18/03/2019

ABSTRACT

Wireless ad-hoc sensor networks are the new milestones in pervasive computing research area. the primary focus of wireless sensor networks was on denial of communication ate certain control levels. The DoC is analyzed generally at medium access control levels. These are kind of resource draining or resource depletion attacks at routing protocol layer. These kinds of attacks can make nodes permanently disable by draining the battery power from nodes by sending a small packet which takes certainly long duration in processing and transmission. Thus, they are named “vampire attacks”. These are not specific in nature. They are reliable on properties of many routing protocols. We came to know that these kinds of attacks are very difficult to detect. They are also very easy to carry out.

Our day-to-day functioning of organizations and people has become intolerable towards organization faults. These faults can overcome by wireless sensor networks. Lack of availability of such networks can result in productivity loss. Availability of these networks should satisfy desired requirements. It is a critical property to maintain consistency between availability and utilization. But, wireless ad-hoc networks are vulnerable to Dos attacks. Research in particular area has been updating day-to-day to enhance survivability of those networks.

Existing architectures and advancements on attempting secure routing, in order to hide the path from discovery, but vampire attacks do not try to change the path from discovery, but vampire attacks do not try to change the path of the packet. They just drain the battery power source from a node. Consideration of routes which benefit the power efficiency is also inappropriate to think, because functionality of such attempts is based on the cooperative node behavior. So, we need to design a system which quantifies the performance of such protocols during an attack. Then only the modification of existing network protocol to withstand the damage caused from attacks during packet transmission is possible.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Background:

Ad-hoc networks have become a major part of the day-to-day operations of many institutions. They have become the primary aid for communication now-a-days. These wireless sensor networks are extremely delicate in nature and hence, are vulnerable to resource depletion attacks which mainly target the networks valuable resources such as the battery power. The main limitations of these networks are the transmission range, battery in the network and communication. Due to such reasons many researchers have been working on designing a secure system which can defend these networks from various attacks.

Wireless sensor networks are sensitive to DoS (Denial of Service) attacks due to the central configuration of the ad-hoc network. Such vulnerabilities of the network affect the availability of these networks to the organizations, which in turn leads to production deficit. One such attack, is the vampire attack, which is generally a resource depletion attack. This attack concentrates mainly on the exploiting the network by targeting its valuable resources such the battery power. This attack slightly varies from both the DoS (Denial of Service) attacks and RoQ (Reduction of Quality) attacks, as it doesn't affect the network right away. It slowly targets the nodes one at a time, draining all their energy, which leads to the shutdown of the entire network.

In order to design a system to defend against the vampire attack, we would have to modify the existing routing protocols. One has to keep in mind that the vampire attacks are not protocol specific. Detecting and preventing such type of an attack is extremely challenging. The attacker can simply generate and transmit large number of unnecessary packets, which increases the processing time as well the energy consumed by the nodes.

1.2 Problem Statement:

The wireless sensor networks, particularly the mobile networks conserve their batteries, as once the batteries are depleted completely, it is very challenging to replace or recharge the batteries. Many mobile networks consist of huge number of nodes and even if one node has its battery depleted, then it affects the entire network. This is what the vampire attacks target. They deplete the individual nodes battery which results in the shutdown of the entire network. It also causes packet loss in the network. In case we detect these vampire nodes and prevent them from affecting the other nodes in the network, then we can save the nodes battery and the entire network indeed.

1.3 Objectives:

The main objectives of this study are:

- Propose an Invasion Discovery Technique to segregate the vampire nodes from the genuine nodes in a mobile ad-hoc network.
- Reshape an existing routing protocol to resist the battery depletion attack.
- Compare the existing and proposed system using performance evaluation metrics such as throughput, packet delivery ratio and end-to-end delay.

1.4 Scope:

The current secure routing protocols namely, SAODV, Ariadne and SEAD are not so sustainable to vampire attacks. The main reason being that the techniques used for the security purpose of defending or withstanding the vampire attacks mainly conflict with those used to secure the routing framework. If we could modify any existing routing protocol to defend against vampire attacks, then we could save the lives of individual nodes as well as the entire network.

1.5 Limitations:

- The vampire attacks are not protocol specific, which make them challenging to detect.
- A lot of protocols which have been investigated, were all vulnerable to these vampire attacks.
- This research study is only applicable for Carousel Attack.

CHAPTER 2
LITERATURE REVIEW

2.1 MANETs:

The compilation of mobile nodes forming a wireless network providing communication to regions where there is no proper communication framework are known as MANETs. [2] They operate without any kind of administrative unit. [1] They are the newly arising technologies which provide the users with the ability to communicate unconcerned of their location and communication facilities available.
Routing protocols are mainly of three types: proactive, reactive and hybrid. They have a crucial position in the framework of MANET and help in discovery new and safe routes to transfer the packets from the source to a destination. The reactive type is known for its on-demand packet delivery which makes it the most used protocol. [3]

2.2 Resource Depletion Attacks:

Such a trending and useful technology also has a drawback. Due to its administration it faces a lot of DOS (Denial of Service) attacks. Mobile ad hoc networks go through two types of attacks. Namely, Routing Disruption Attack and Resource Depletion Attack. Resource Depletion Attacks are those attacks in which the main the concentration of the attacker would be the resources of the network such as the energy of the nodes or memory. Whereas the Routing Disruption Attack is a type of attack which tries to change the path set by the routing table. Examples of such an attack are the Wormhole attack and Sybil attack. Vampire attacks come under the Resource Depletion Attacks as they drain the energy of the nodes. Vampire attacks don't deny the service instantly, they work slowly by draining each and every nodes energy and then completely shut down the network. [4] Detecting a vampire attack is a very complex process. They are not protocol specific.

2.3 Vampire attack:

Vampire attack is a type of resource depletion attack in which a malicious node creates and sends messages through a longest path which consumes more energy and slowly results in the depletion of battery life.

The attack can happen on both Stateless Protocols and Stateful Protocols.

2.3.1 Stateless Protocols:

In Stateless Protocols the intermediate nodes don't make any decisions. The complete route is predefined by the source node and attached within the packet header.

2.3.2 Stateful Protocols:

Unlike in stateless protocols, here the intermediate nodes can make forwarding decisions. They have complete knowledge of the forwarding decisions, topology, etc.

2.4 Attacks on Stateless Protocols:

2.4.1 Carousel attack:

In this attack, the packet repeatedly reaches the same set of nodes forming a series of loops as shown in the image below. In this attack, the adversary purposely introduces packets with loop chains. Carousel attack targets the source routing protocols.

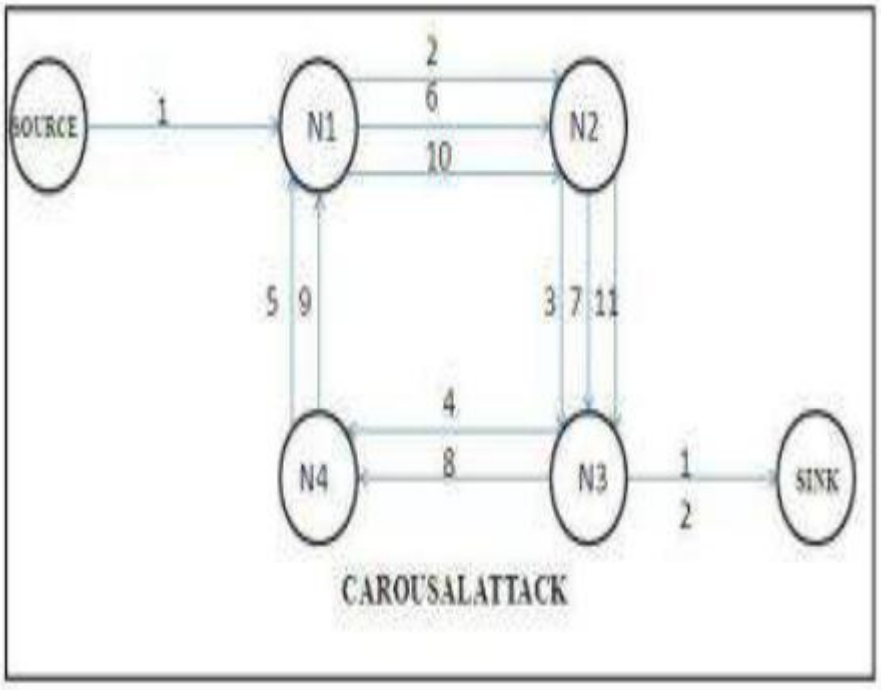


Figure 2.1: Carousel Attack [35]

2.4.2 Stretch Attack:

In stretch attack, the adversary makes the packet travel in longer paths trying to include all the nodes in the network. This consumes more energy when compared to that of the honest path. The packets are made to cover a greater number of nodes than the optimal number of nodes.

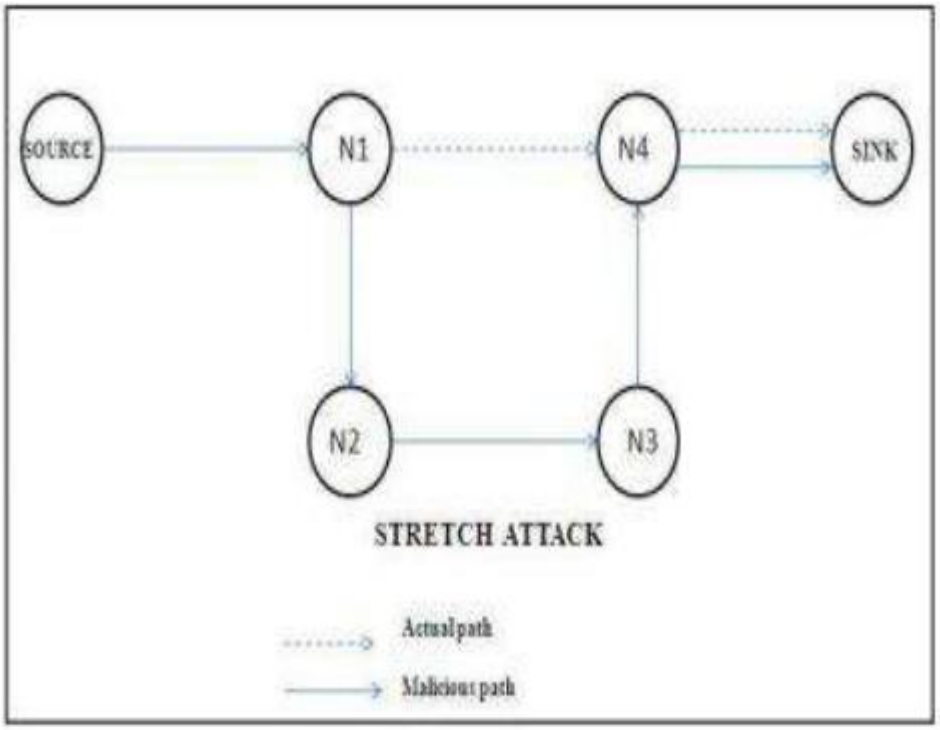


Figure 2.2: Stretch Attack [35]

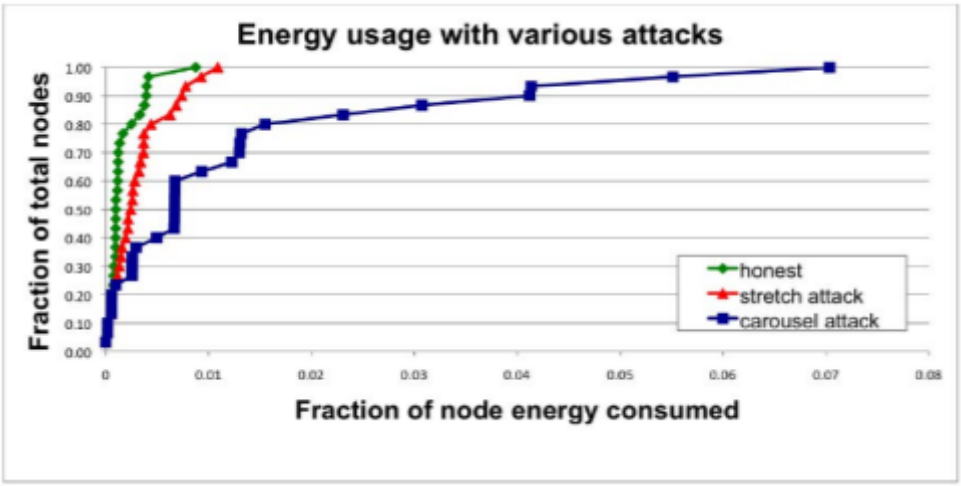


Figure 2.3: Graphical representation of energy drain for various attacks [36]

2.5 Related Works:

The structure less property is the main parameter which makes the ad hoc networks vulnerable. Many researchers have dedicating their lives in strengthening the survivability of an ad hoc network. Now, coming to the drawbacks of the existing system being used for

the prevention of vampire attacks, the attestations added to the packet header increase the size of the packet to be processed. The attestation in other words is like a signature made by each and every node the packet passes through. The nodes cannot alter the data written by the previous nodes. But, due to the data added on by each and every node, the size of the packet increases and becomes difficult while processing the packet i.e., during coding, encryption and decryption. One solution for this can be by adding a flag field in header which is always zero and becomes one when the same packet reaches a particular node again. [5] This way the size of the header doesn't increase too much.

Few researchers discuss about the Denial of sleep attack in wireless sensor networks in one of their papers. This is a type of Denial of Service (DOS) attack. The main interest of this type of attack is the energy in the network. They drain the power from few nodes and it is really a challenge to replace those battery-drained nodes. A solution for this attack was proposed- to welcome transmissions only from genuine nodes. To regulate this process of transmission of sleep deprivation packets, Zero Knowledge Protocol (ZKP) was used. Then the interlock protocol was implemented during the key exchange for greater security. [6] Just like the Denial of Sleep attack, the Vampire attacks also are a great deal to handle. Even they target the battery power of a network. The slowly drain the energy of the network by attacking the nodes one-by-one. To prevent the such a vampire, Distance Vector routing protocol can be used. The reason being that this protocol contains of very prominent algorithms such as the Link-State Algorithm and Distance Vector routing Algorithm. [7] The Denial of service (DOS) attacks can operate on any layer of the network. When DOS takes place, a certain node refuses to supply necessary aid to the remaining genuine nodes. In order to maximize or improve the sustainability of a network, an end-to-end authentication and two-threshold value can be applied to detect these attacks. We can also make use of the required performance analysis to maximize the elasticity and accuracy of a particular detection system. [8][9][10]

As per few research articles, the Vampire attack can be detected and prevented by using a specialized protocol such as Energy Weight Detection Algorithm (EWDA) and a routing algorithm. When a particular nodes energy reaches the threshold, it is considered as malicious. Then a safe route is established to transmit the packets to the destination. For this a Routing Algorithm is used. First, trust values are assigned to each and every node. The node which is malicious will have a trust value of 0 and the genuine node will have a value of 1. So, while constructing a secured route, all the nodes with a trust factor of 1 are assigned for the packet delivery and all the nodes with a value of zero are excluded. [11]
Wireless Sensor networks have many applications these days. They are being used by the armed forces to broadcast classified information through a wireless network and the central government of many countries is using WSN's for nationwide protection to keeping an eye on the borders and to discover any kind of terrorist attacks. A vampire attack can be induced in two ways: External attack and Internal attack. The carousel attack come under the external attack, where a node with high battery power is considered, so that it can have

an extra life. Whereas the Internal attack is induced using a node within the network range, which is usually a trusted node in the network. It is deployed by modifying the existing routing protocol. One thing to be noticed is that distinguishing the malicious node from the genuine node is quite harder in the case of an internal attack when compared to that of an external attack. The malicious nodes in this case have the same features and look alike when compared to the normal nodes. Their battery life, power of transmission, everything is just like that of a genuine node in the network. This is the main reason for facing challenges while discovering a malicious node in an internal attack. [12]

A lot of renowned researchers have been working on the effects of vampire attacks on wireless ad hoc networks. They have investigated of each and every detail about how the attack is deployed into the network, how it affects the network and have introduced many detection and prevention techniques for this attack. One such research was conducted, where they have discussed all the effects of vampire attack on "Dynamic State Routing Protocol (DSP)" & "Destination Sequenced Distance-Vector Routing (DSDV) protocols".[13] They have even proposed new systems to detect and prevent these types of resource exhaustion attacks. Few researchers have been using Cluster Head in order to withstand the effects of a vampire attack. The cluster head takes charge during the vulnerable times and helps in the safe delivery of packets from the source to destination, resulting in zero packet loss. [14]

In the research work titled "Vampire attack detection and prevention using DLWASN on wireless adhoc sensor network" they have proposed a protocol named DLWASN for the prevention of vampire attack. This protocol applies hash algorithm for cryptographic function. The performance analysis was of the proposed system was done based on few criteria's such as throughput, packet drop, delay, etc. [15]
An Elliptic Curve Cryptography (ECC) algorithm was proposed by one of the researchers. They have customized Clean Slate Protocol and proposed Valuable secure protocol (VSP). Key management phase is one the three phases in clean state protocol, which is used for encrypting the data in order to protect the wireless nodes and valuable information in the network. But, the size of the key is a bit large, making it to take extra processing time and in turn leading to delay in the network. So, here we need a smaller key, which is supplied by the Elliptic Curve Cryptography (ECC). This algorithm a customized version of the clean slate protocol. [16]

Rivest, Shamir, Adleman (RSA) algorithm has been used in some of the recent works, where the Ad Hoc On-Demand Vector routing protocol (AODV) was used in the research to study the effects of vampire attack on it. The original energy levels in the network without a malicious node were compared with the energy levels during the vampire attack and after the prevention of the attack. Jose Anand and K. Sivachandar have chosen few AODV operatives to assess based on energy levels in the network. [17] The RSA algorithm has been used to survey, assess and evaluate on how the vampire attack

influences the AODV protocol. It provides protection for all the nodes in the network from the resource depletion attack.

The prevention for vampire attack can also be done by a simple approach of packet surveilling. RREQ (Route Request) packets are sent from the source to destination, where they pass through all the nodes in the network. But the destination receives the packets only from the genuine nodes and drops all the packets from the malicious nodes. The nodes examine the packet header in contrast to the received RREQ message for accessing the data like location of the destination and simulation id. Then they set up a safe route for the packet delivery to the destination. But one drawback of such a system is that the simulation speed falls low as the number of nodes in the network increases. [18]

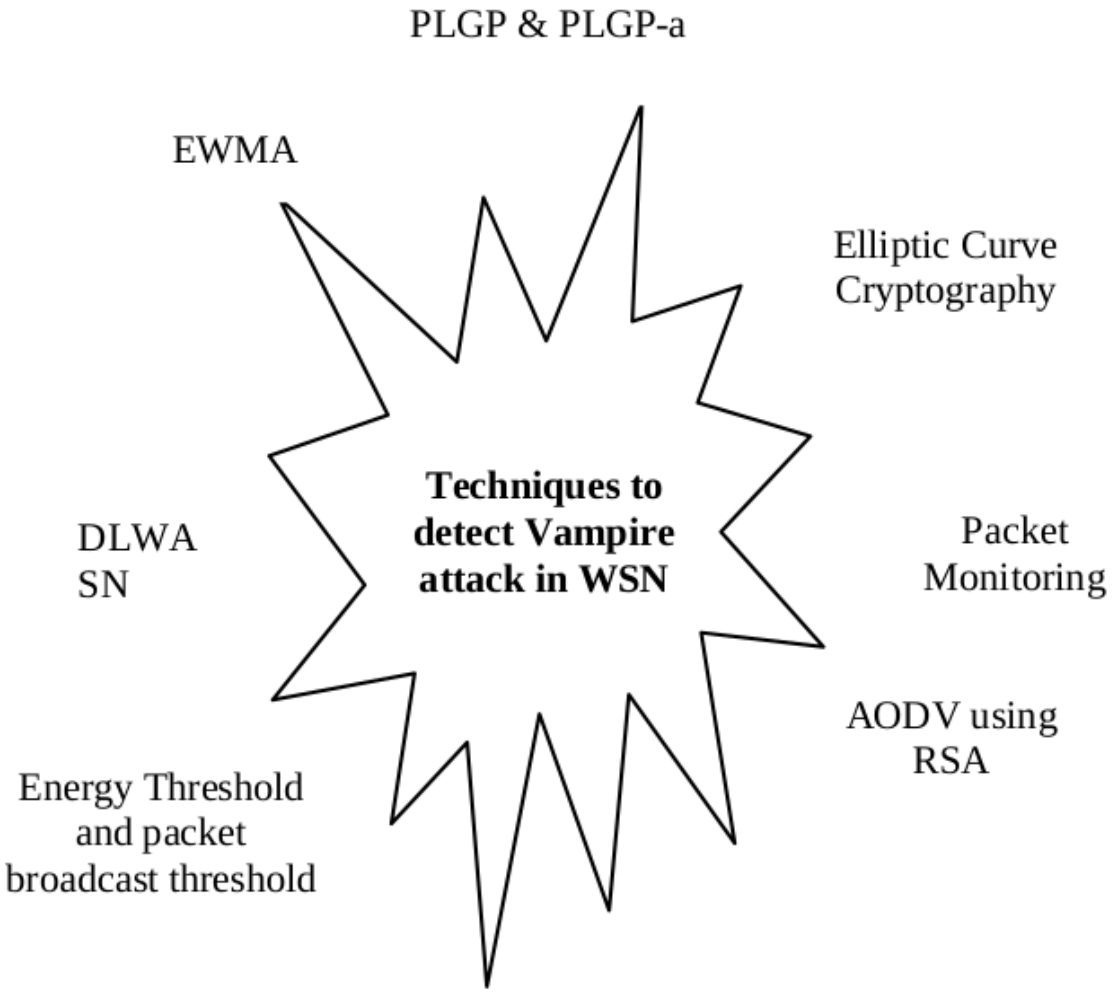


Figure 2.4: The existing techniques present for the invasion discovery and prevention of Vampire Attacks [19]

CHAPTER 3
METHODOLOGY

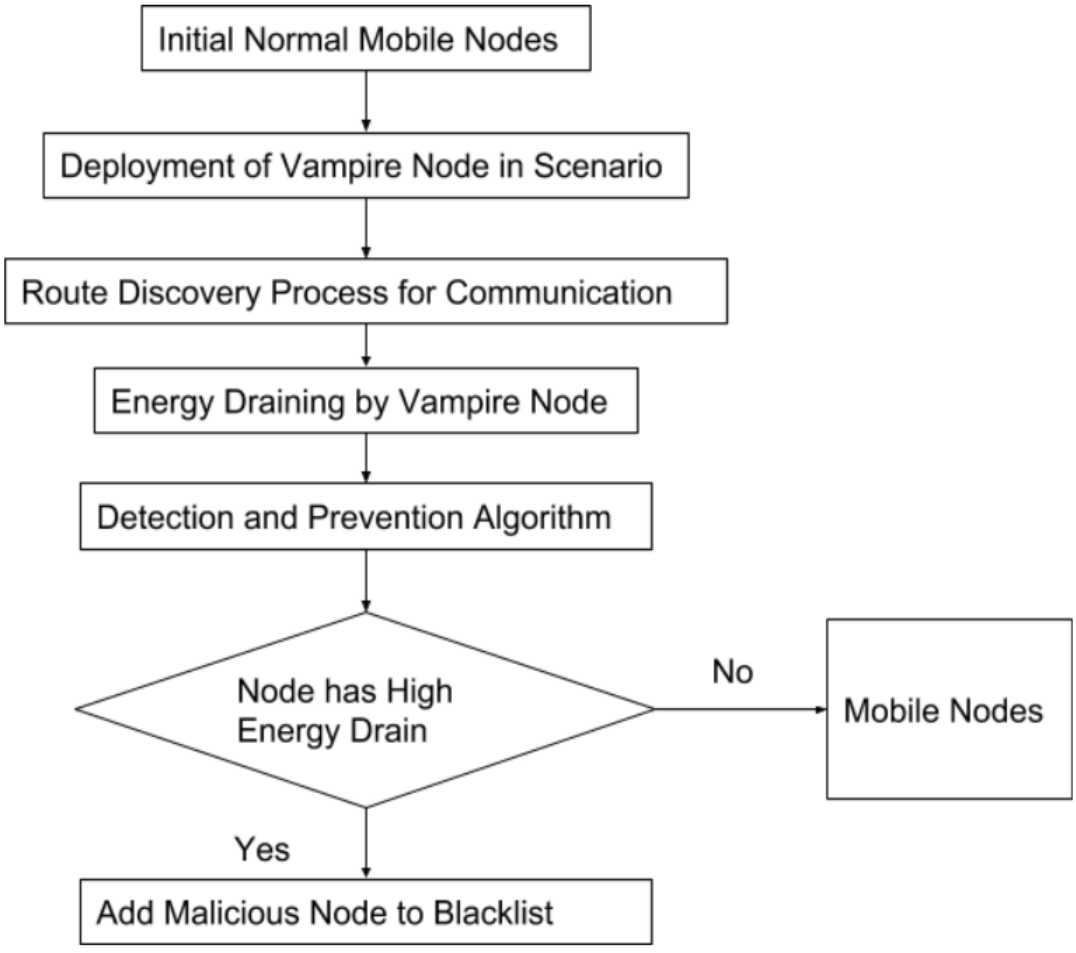
3.1 Intrusion Detection System:

3.1.1 Proposed system:

Detection technique to identify malicious node(s) into ad-hoc networks:

The most essential step in the proposed system is to witness the energy drain and time taken to process the packet at each and every node in the network. The next step is to observe the energy depletion after the deployment of malicious node and the proposed system for detection and prevention in order to evaluate the alteration in energy drain.

3.1.2 Flow Chart:



Step 1: Transmit a Route Request Packet (RREQ) from the source node to all the nodes in the network in order to check for the shortest path of communication.
Step 2: The source receives the Route Reply message (RREP) from the destination.
Step 3: Take a look at the energy levels of all the nodes present in the network as well as the time taken by each node to process the packet. The malicious node will have the highest energy drain and time taken when compared to the other nodes. The remaining nodes will all have the same energy drain.
Step 4: If a particular node has highest energy drain
4.1 Detection
Check the routing table for the node id of the suspicious node.
4.2 Prevention
Label the node as malicious node and try to find a honest path to securely deliver the message.
Step 5: Else, incase all the nodes are having similar energy drain, then we have to consider all the nodes as legitimate nodes.
Step 6: Stop

3.2 Protection from Vampire Attack:

This can be done by the modification of existing sensor network routing protocol.

3.2.1 PLGP in presence of vampires:

When the packet is transmitted from the source, it has to pass through the intermediate nodes in order to reach the destination. These intermediate nodes have no knowledge about the path in which the packet has to travel. So, the packet can be redirected to any corner of the system of nodes. The malicious node can easily divert the packet from the desired route.

3.2.2 Security against vampire attacks:

3.2.2.1 No-backtracking property:

`The no-backtracking property is said to be fulfilled, when a packet passes through same number of hops either a malicious node is present or not. The energy consumed throughout the network is same whether the vampire is present or not. The activities of the malicious nodes do not have any effect.
Case 1: L is honest L...(hops) ...D
Case 2: L is Malicious L...(hops) ...D

If we can satisfy no-backtracking, then we can provide protection against vampire attack. The existing PLGP system cannot satisfy no-backtracking. The intermediate nodes are not aware of the path history of a packet. They can forward the packet to any corner of the network, which makes the PLGP system sensitive to vampire attacks.

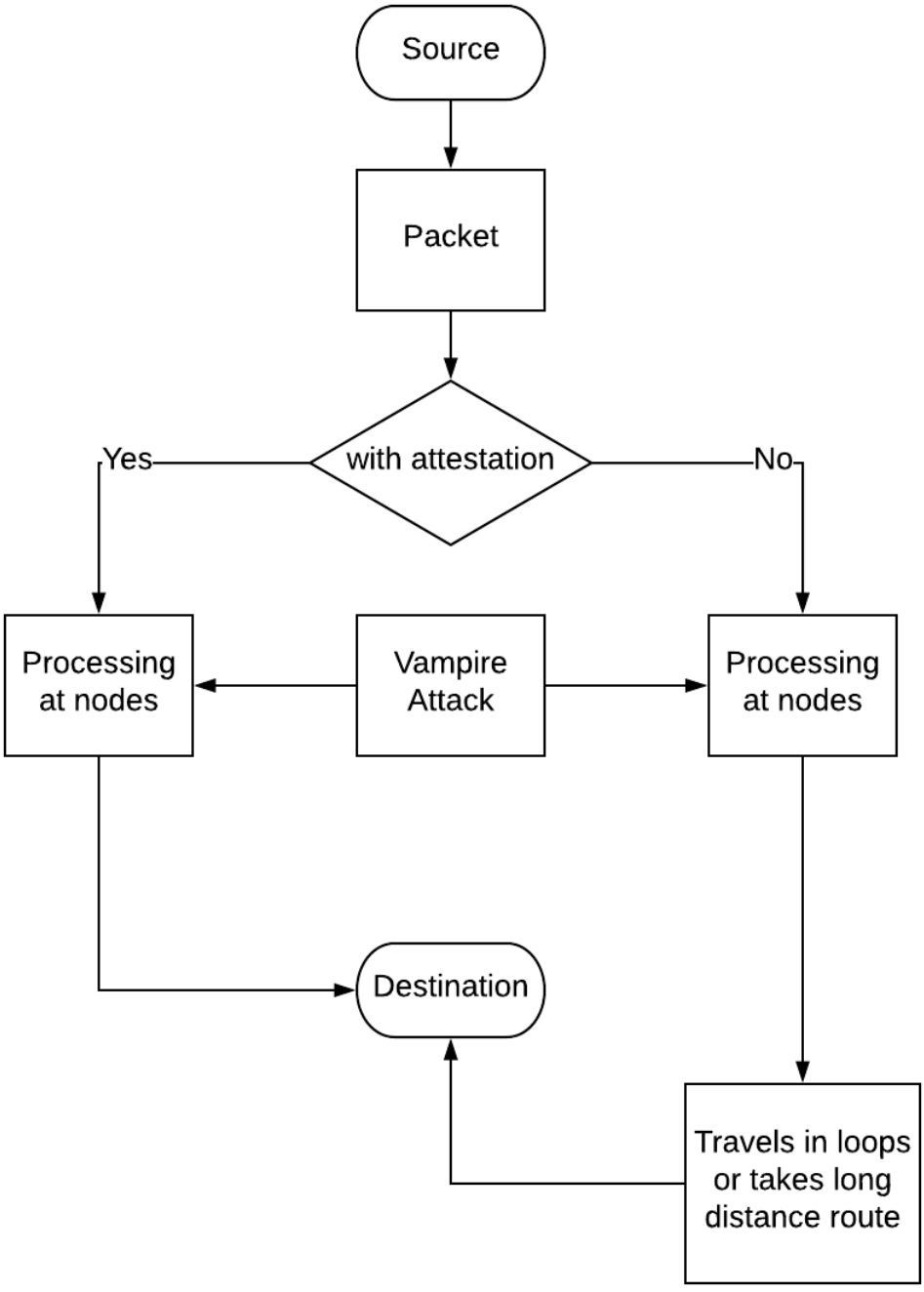
3.2.3 Proposed system:

3.2.3.1 Propose PLGP with attestations (PLGPa):

Each and every packet delivered from the source will have an attestation in its header, where the address of the destination is attached and also the path history of the packet will be stored. Each node the packet travels will have its signature stored in the packet header, which forms a series of signatures. Every node the packet passes through next will verify this path history and forward it to the safe route. These signatures will help the packet from not reaching the same node again and again.

A network is said to be safe from vampire attack when it satisfies No-backtracking. A packet has to have same number of hops whether a malicious node is present or not. In order to satisfy No-backtracking a valid route is hooked up to the route authentication.

3.2.4 Flow Chart:



3.3 Performance Evaluation:

The proposed system is developed and implemented using NS2 and the system performance has been evaluated using parameters mentioned below :

3.3.1 Throughput:

Throughput is the number packets that have been received by the destination successfully in a given time period.

$$\text{Throughput [pps]} = \frac{\text{Number of received packets}}{\text{Data transmission period}}$$

3.3.2 End-to-end Delay:

End-to-end delay is defined as the average time consumed by a packet to travel from the packet creator to the packet destructor. It is calculated from when the packet arrives in queue. So, even the waiting period at queue is also included. It even considers the time taken for the route discovery process.

It is formulated as:

$$\text{End-to-End Delay [ms]} = \frac{\text{Data Transmission Period}}{\text{Number of received packets}} * 1000$$

3.3.3. Packet Delivery Ratio:

Packet Delivery Ratio indicates the ratio of number of packets which make to destination safely to the number of packets produced at the source.

$$\text{PDR} = \frac{\text{Sum of number of packets received}}{\text{Sum of number of packets sent}} * 100$$

3.4 Simulation Parameters:

Table 3.1 Simulation Parameters

Channel	Channel/WirelessChannel
Propagation	Propagation/TwoRayGround
Network Interface	Phy/WirelessPhy
Platform	Ubuntu 18.04
NS Version	Ns-allinone-2.35
MAC	Mac/802_11
Interface Queue	Queue/ DropTail / PriQueue
Link Layer	LL
Antenna	Antenna/OmniAntenna
Interface Queue Length	50 packets
No. of Nodes	10, 30, 50, 100, 150
Max Speed of Nodes	5 m/s
Simulation area size	500*500
Traffic Pattern	CBR Sessions
Packet Rate	60 pps
CBR Packet Size	64 bytes
Simulation Duration	20.0 seconds

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Performance Evaluation:

The proposed system has been developed and implemented using NS2. The performance evaluation of this research has been done on the basis of the following parameters :

4.1.1 Throughput:

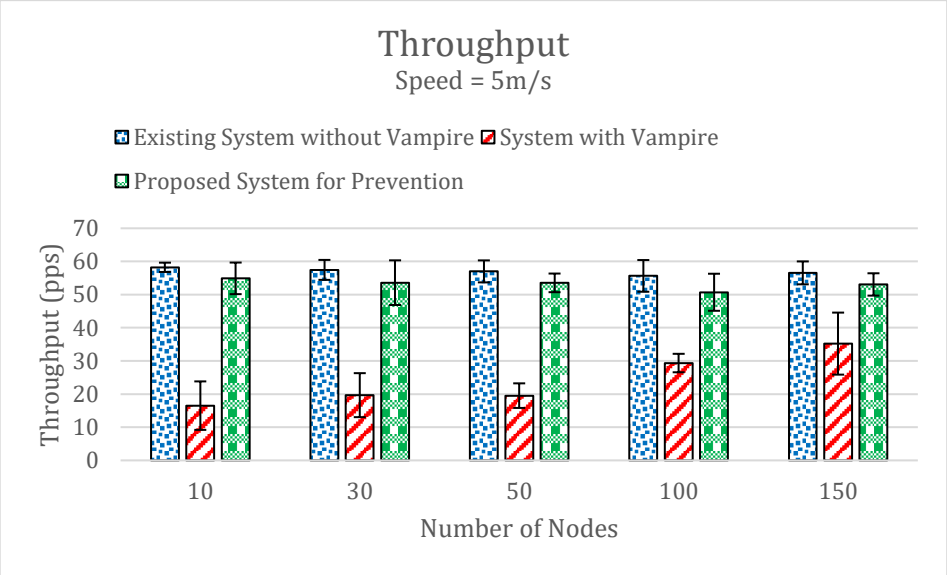


Figure 4.1 Graph for Throughput vs No. of nodes, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

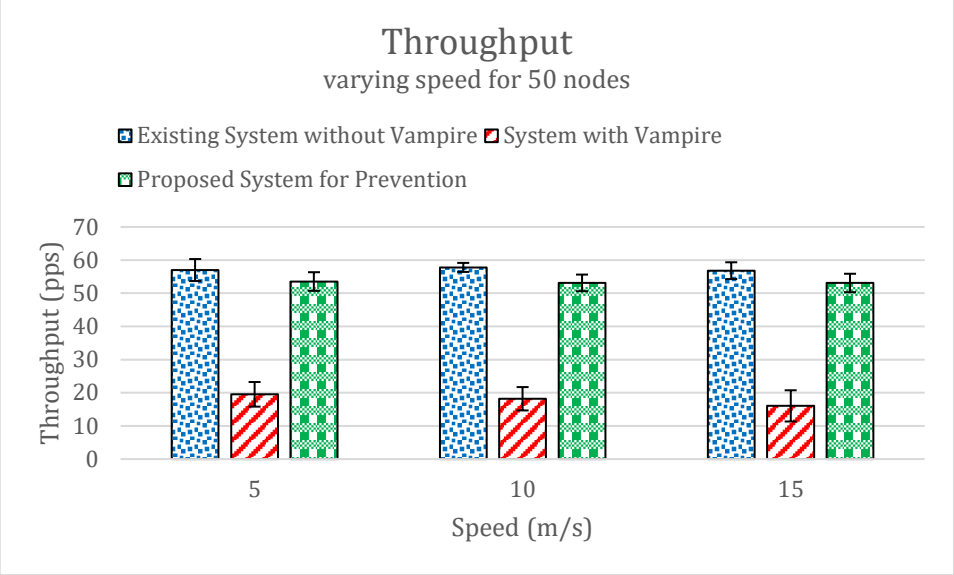


Figure 4.2 Graph for Throughput vs Speed, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

From the above graph of figure 4.1, we can observe that by deploying 10, 30, 50, 100 and 150 nodes at speed of just 5m/s, the throughput results obtained for the proposed system are better than that of the vampire attack scenario. Then from the figure 4.2, when the nodes attain a speed of 5, 10 and 15 m/s, the Throughput results observed in the case of the proposed system have improved when compared to that of the vampire attack, but not as much as the existing system. This is because, when the speed of the nodes increases the congestion and establishing a connection to destination gets quite difficult.

4.1.2 Packet Delivery Ratio:

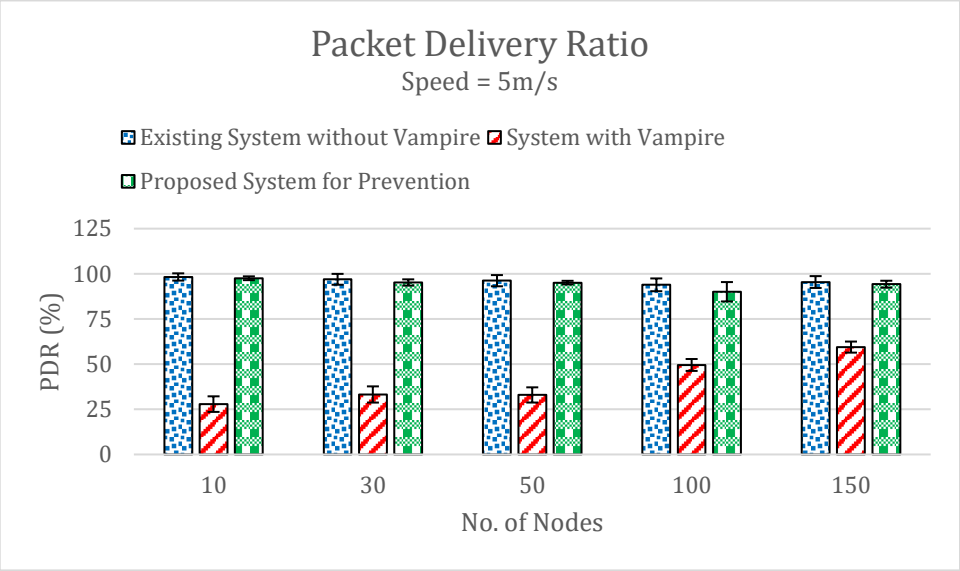


Figure 4.3 Graph for Packet Delivery Ratio vs No. of nodes, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

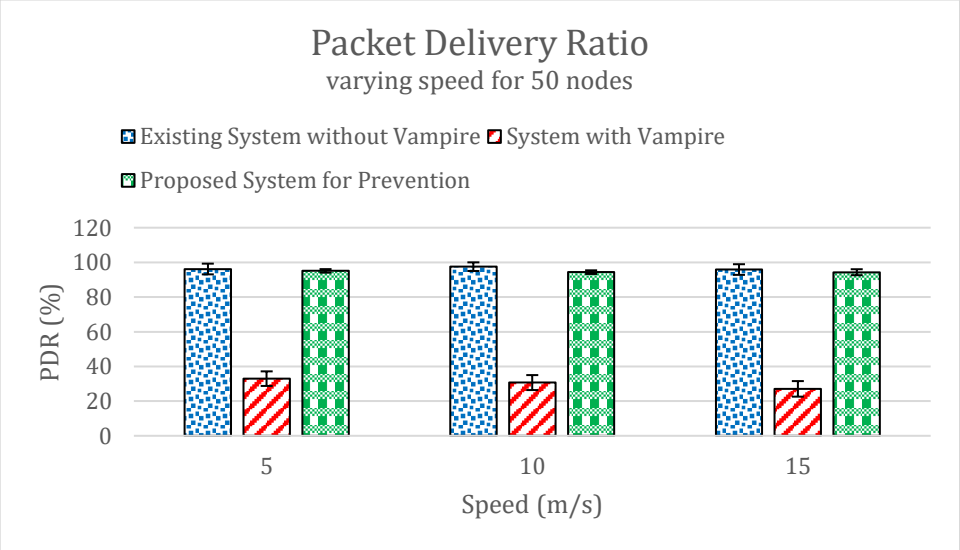


Figure 4.4 Graph for Packet Delivery Ratio vs Speed, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

From the above graph in figure 4.3, we compare three categories of nodes functioning under the existing system, vampire attack and under the proposed system where we try to mitigate the vampire attack. The nodes considered here are considered to have a speed of just 5m/s. The Packet delivery ratio of the proposed system is observed to be better than that of the vampire attack. Then from the figure 4.4, where the nodes are assigned a speed

of 5, 10 and 15 m/s, the packet delivery ratio in case of the proposed is observed to be improving than the vampire attack, but not as much as the existing system because, as the speed increases, connection establishment between nodes also gets quite difficult.

4.1.3 End-to-End Delay:

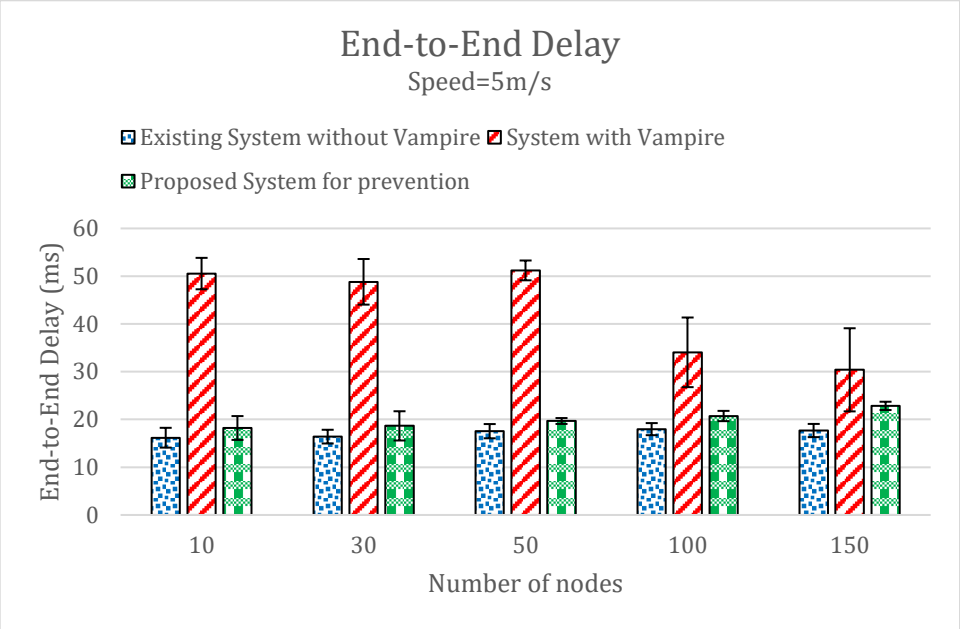


Figure 4.5 Graph for End-to-end Delay vs No. of nodes, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

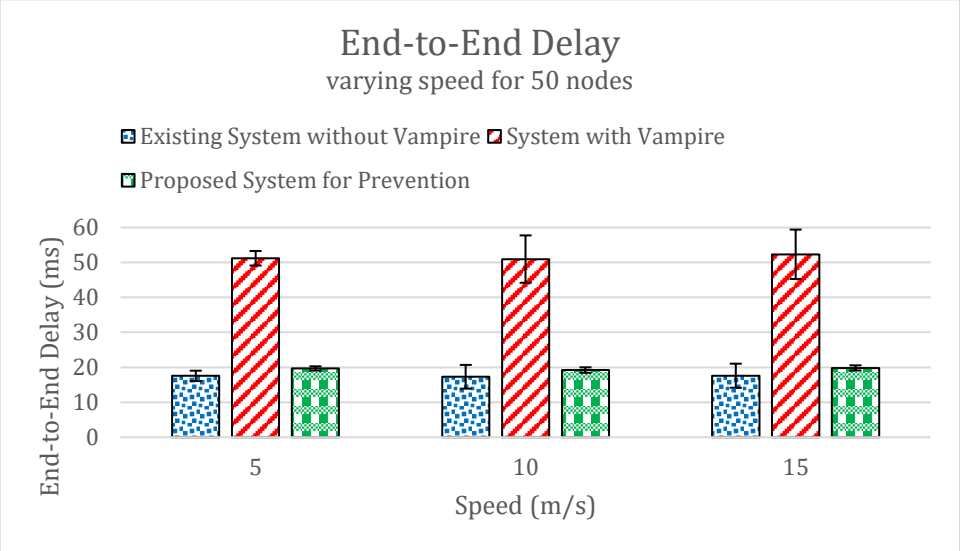


Figure 4.6 Graph for End-to-end Delay vs Speed, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

From the above graph in figure 4.5, we can observe the comparison of 10, 30, 50, 100 and 150 nodes with a speed of just 5m/s, under three categories of existing system, vampire attack and proposed system. The end-to-end delay is observed to be lessening in the case of proposed system when compared with the vampire attack, but not as much as that of the existing system. The main reason for this is that we are adding an attestation to the packet header in the proposed system, due to which the size of the packet will increase a little bit. This results in consuming a little more time for processing the packet. Hence, the delay in proposed system is a little higher when compared to that of the existing system. The same can be observed in the figure 4.6, depicting the graph for end-to-end delay plotted by varying the speed.

4.1.4 Average Energy Consumed by all the Nodes:

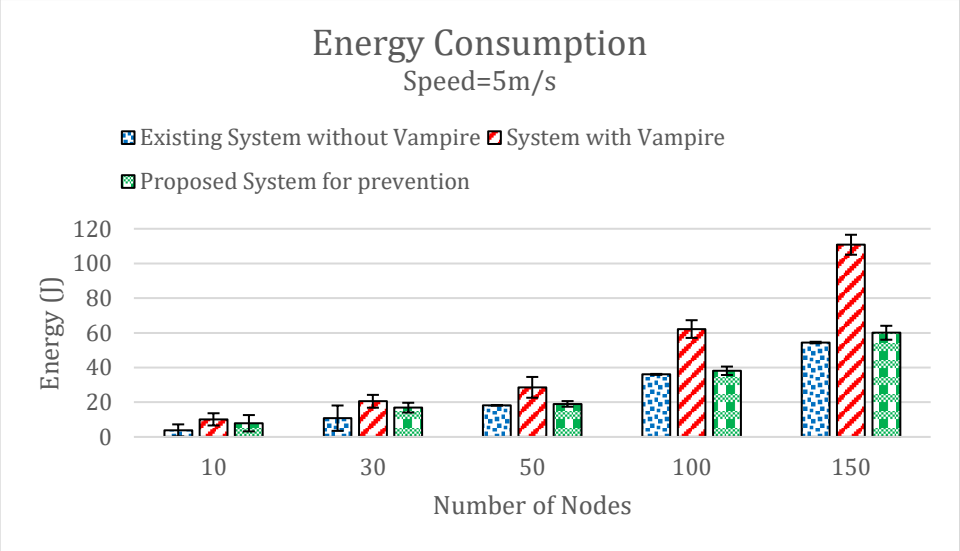


Figure 4.7 Graph for Energy consumed vs No. of nodes, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

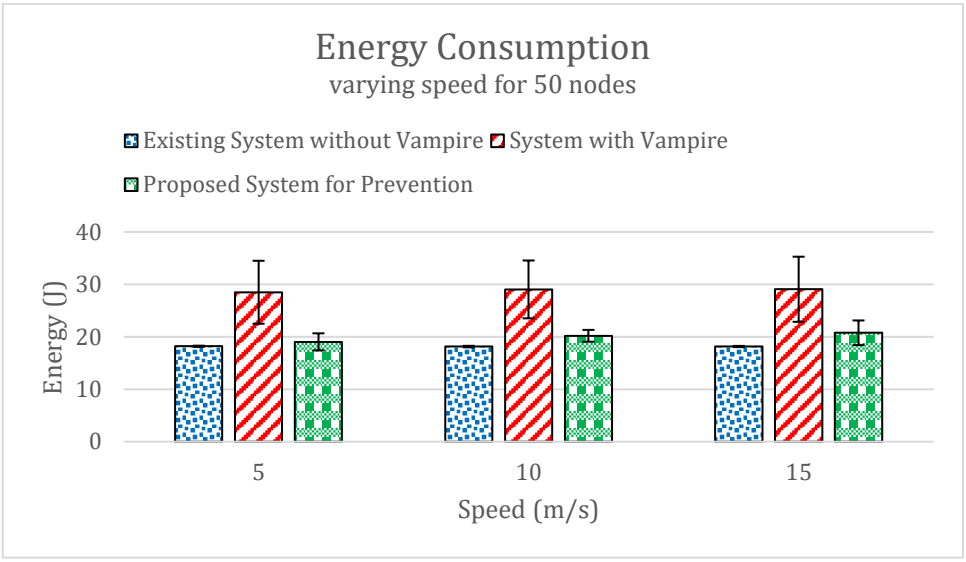


Figure 4.8 Graph for Energy consumed vs Speed, comparing the performance of three categories: Existing system, Vampire attack and proposed system.

CHAPTER 5
CONCLUSION

In this research study, we described a Resource Depletion Attack known as the vampire attack. These types of attacks are not specific to any protocol. Vampire attacks can be distinguished as: Carousel and Stretch Attack. Our proposed system designed for the discovery of malicious nodes, depends upon energy drain in the network. Then, to prevent the vampire attack, all the packets are attached with an attestation in the header, where the packet gets signatures from each and every node that it passes through. This prevents the packet from reaching the same nodes again and again. The proposed system is developed and implemented using NS2 and the system performance has been evaluated using parameters such as throughput, packet delivery ratio and end-to-end delay. The performance evaluation has been done by using mobile nodes. All the performance parameters have proved that the proposed system is efficient in detecting and preventing the vampire attack.

REFERENCES:

1. Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.
2. Han, S. Y., & Lee, D. (2013). An adaptive hello messaging scheme for neighbor discovery in on-demand MANET routing protocols. IEEE communications letters, 17(5), 1040-1043.
3. Pandey, S., Prakash, V., & Yadav, S. QOS Optimization of Multipath Routing in MANET.
4. Vijayanand, G., & Muralidharan, R. (2014). Overcome vampire attacks problem in wireless ad-hoc sensor network by using distance vector protocols. International Journal of Computer Science and Mobile Applications, 2(1), 115-120.
5. Garg, A., & Sharma, M. K. (2015). Detection and Prevention of Vampire Attack in MANET. International Journal on Recent and Innovation Trends in Computing and Communication, 3(12), 6793-6798.
6. Naik, S., & Shekokar, N. (2015). Conservation of energy in wireless sensor network by preventing denial of sleep attack. Procedia Computer Science, 45, 370-379.
7. Vijayanand, G., & Muralidharan, R. (2014). Overcome vampire attacks problem in wireless ad-hoc sensor network by using distance vector protocols. International Journal of Computer Science and Mobile Applications, 2(1), 115-120.
8. Luan, L., Fu, Y., & Xiao, P. (2012). An effective denial of service attack detection method in wireless mesh networks. Physics Procedia, 33, 354-360.
9. Roy, D., & Verma, S. Vampire Attacks: Detection And Prevention.
10. https://en.wikipedia.org/wiki/Ns_(simulator)
11. Roy, D., & Verma, S. Vampire Attacks: Detection And Prevention.
12. Sharma, M. K., & Joshi, B. K. (2017, August). Detection & prevention of vampire attack in wireless sensor networks. In Information, Communication, Instrumentation and Control (ICICIC), 2017 International Conference on (pp. 1-5). IEEE.
13. Pawar, D. D., & Singh, M. (2016). Prevention of Vampire Attacks in Wireless Sensor Network. International Journal of Computer Applications, 154(9).
14. Choukiker, L., Saxena, A., & Manoria, M. (2016). Vampire Attack Prevention to reduce Node Power Consumption in WSN. System, 133(11).

15. Pawar, P. P., & Uke, S. N. (2014). Vampire attack detection and prevention using DLWASN on wireless adhoc sensor network. Int. J. Res. Comput. Sci, 1(03), 10-13.
16. Vanitha, K., & Dhivya, V. (2014). A valuable secure protocol to prevent vampire attacks in wireless ad hoc sensor networks. In IEEE international conference on innovations in engineering and technology (ICIET'14) (Vol. 3).
17. Anand, J., & Sivachandar, K. (2014). Vampire attack detection in wireless sensor network. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume, 3.
18. Shrivastava, A., & Verma, R. (2015). Detection of vampire attack in wireless ad-hoc network. Int. J. Softw. Hardw. Res. Eng, 3(01), 43-48.
19. Juneja, V., & Gupta, D. V. (2017). Strategies for Detection and Prevention of Vampire Attack in WSN. International Journal of Advances in Computer and Electronics Engineering, 2(2), 13-16.
20. The network simulator — ns-2. http://www.isi.edu/nsnam/ns/.
21. Aad, I., Hubaux, J. P., & Knightly, E. W. (2004, September). Denial of service resilience in ad hoc networks. In Proceedings of the 10th annual international conference on Mobile computing and networking (pp. 202-215). ACM.
22. Acs, G., Buttyan, L., & Vajda, I. (2006). Provably secure on-demand source routing in mobile ad hoc networks. IEEE transactions on Mobile Computing, 5(11), 1533-1546.
23. Aura, T., Nikander, P., & Leiwo, J. (2000, April). DOS-resistant authentication with client puzzles. In International workshop on security protocols (pp. 170-177). Springer, Berlin, Heidelberg.
24. Bellardo, J., & Savage, S. (2003, August). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In USENIX security symposium (Vol. 12, pp. 2-2).
25. Bernstein, D. J., & Schwabe, P. (2008, December). New AES software speed records. In International Conference on Cryptology in India (pp. 322-336). Springer, Berlin, Heidelberg.
26. Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.
27. Blake, I. F., Seroussi, G., & Smart, N. (1999). Elliptic Curves in Cryptography, volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge.
28. Osvik, D. A., & Stefan, D. (2014). Fast Implementations of AES on Various

Platforms.

29. Chan, H., Perrig, A., & Song, D. (2003, May). Random key predistribution schemes for sensor networks. In Security and Privacy, 2003. Proceedings. 2003 Symposium on (pp. 197-213). IEEE.
30. Chang, J. H., & Tassiulas, L. (2004). Maximum lifetime routing in wireless sensor networks. IEEE/ACM Transactions on networking, 12(4), 609-619.
31. Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol (OLSR) (No. RFC 3626).
32. Deng, J., Han, R., & Mishra, S. (2005, November). Defending against path-based DoS attacks in wireless sensor networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (pp. 89-96). ACM.
33. Deng, J., Han, R., & Mishra, S. (2006). INSENS: Intrusion-tolerant routing for wireless sensor networks. Computer Communications, 29(2), 216-230.
34. Doshi, S., Bhandare, S., & Brown, T. X. (2002). An on-demand minimum energy routing protocol for a wireless ad hoc network. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3), 50-66.
35. https://www.slideshare.net/augustinjose7/vampire-attacks
36. Vasserman, E. Y., & Hopper, N. (2013). Vampire attacks: draining life from wireless ad hoc sensor networks. IEEE transactions on mobile computing, 12(2), 318-332.