International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072

Anomaly Detection through Firewall Policies and Vampire Attacks

BharathyVijayan

Mtech Computer Science And Engineering
LourdeMatha College Of Science And Technology
Trivandrum,India

Abstract- ***Network survivability is the ability of a network keeping connected under failures and attacks, which is the most important issue in the design and performance of wireless ad hoc sensor networks. This paper explores resource consumption attacks called "Vampire" attacks which permanently disables the whole network by quickly draining nodes battery. Detecting vampire attacks in the network is not an easy task. A simple vampire present in the network can increase the network wide energy usage. These vampire attacks are not protocol specific, but rather rely on the properties of many popular classes of routing protocols. The paper projects its focus on the way in which the attack can be overcome in the best possible way. On the basis of a rule based classification, detection of anomalies is done in a better manner. The proposed system describes the detection of anomalies through firewall policies and vampire attacks and thus make the network live. This enhanced workincreases the quality of service in the network and it will regulates all the nodes activity in the network.***

Key words : *Denial of service, security, routing, ad-hoc networks,sensor networks, wireless networks,etc...*

1.INTRODUCTION

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Sensors are spread in an environment without any predetermined infrastructure and cooperate to execute common monitoring tasks which usually consist in sensing environmental data from the surrounding environment. Ad-hoc Wireless Sensor Networks consist of sensors which are distributed in an ad hoc manner. The sensor nodesperforms the sensing tasks. These are

interconnected with the wireless links. Every sensor is operational with some sensing, processing and communication components. Thus, when some event occurs (to be captured by sensor) it generates a report. This report is then forwarded to the sink; by some routing path over the network. Nowadays, Wireless sensor network is part of our day to day life.Adhoc mode is a method for wireless devices to directly communicate with each other. Operating in adhoc mode allows all wireless devices within the range of each other to discover and communicate in peer to peer fashion without involving central access points. An adhoc wireless sensor network is a decentralized type of wireless network. The network is adhoc because it does not rely on any pre-existing infrastructure,suchas router in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data to other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. An adhoc network tends to feature a small group of devices all in very close proximity to each other. An adhoc network can also be defined as any set of networks where all devices have equal status on a network and are free to associate with any other adhoc network device in link range. Ad hoc network typically refers to a mode of operation of IEEE802.11 wireless networks.

Wireless networks are vulnerable to security attacks. This is due to the broadcast nature of the transmission medium.Wireless sensor networks are susceptible to attacks and threats such as eavesdropping or passive information gathering,node malfunctioning, denial of service(DoS),malicious discovery attack and many more. WSNs are highly vulnerable to the DoS attacks because of their Ad-Hoc nature. A great deal of research has been done to increase the survivability of these networks.The longest DoS attack will drain the batteries of all nodes. In this type of resource depletion attack, the focus of attack is on the battery power. As battery is one of the main resource of any sensor node,such battery depletion attack is always dangerous as it drain all the power of the network.So preventing such attacks is very necessary. During attacks by malicious nodes, the node's energy expenditure increases drastically thereby leading to its energy depletion making the node incapable of transmission in future. Energy is one of the most precious

resource for sensor networks. Communication is especially expensive in terms of power. The battery power consumption attacks at routing layer protocol will completely disable networks by depleting node's battery power and is defined as vampire attacks. These attacks never flood the network with large amount of data, instead it drains node's life by delaying the packets.

Vampire attack means creating and sending messages by malicious node which causes more energy utilization by the network leading to slow reduction of node's battery life.This attack is not particular to any protocol. These attacks also do not rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution.Since vampires use protocol compliant messages, these attacks are very difficult to detect and prevent.

1.1 PROBLEM OBJECTIVE

The objective of this paper is to formulate an anomaly detection method through vampire attacks and firewall policies that helps to deplete the energy consumption of adhoc wireless network and increases the network lifetime.

1.2 PROBLEM MOTIVATION

The life of the wireless adhocsensor network depends on nodes battery power.But batteryrecharging or replacing is impossible in most of the application.As a result power drainage will leads to the failure of the node and it will also affect the network.Sometimes data loss may also occur. Therefore an efficient energy utilization scheme is required.It means that data packets should be transmitted by using minimum units of energy.But some malicious packets called vampire packets may consume more energy for packet forwarding than that of honest packet forwarding .This will lead to power drainage of node and network failure. If it is possible to find and avoid these type of malicious packets, then we can increase the life of the node and thereby the network.This inturn will be very crucial in many of the situations and will increase the wide acceptability of adhoc wireless networks in many important applications.

2.RELATED WORK

Michael Brownfield [1] discussed the energy resource vulnerabilities at MAC level. Denying sleep effectively attacks each sensor node's critical energy resources and rapidly drains the network's lifetime.So a new GMAC protocol is proposed to control the sleep awake pattern of sensor nodes. G-MAC has several energy saving features which not only show promise in extending the network lifetime, but the centralized architecture makes the network more resistant to denial of sleep attacks. This scheme performs well in all traffic situations but deals only with MAC layer depletion attack.

FatmaBouabdullah, NizarBouabdullah, RaoufBouabdullah [2] proposed a cross layer strategy that considers routing and MAC layers jointly. A network lifetime is time for the first node in wireless sensor network to fail. An efficient routing protocol would drain energy slowly and uniformly among nodes leading to the death of all nodes nearly at same time. At routing level they proposed that sending data through multiple paths instead of using a single path so can balancing energy consumption. At MAC level limits the retransmission over each wireless links according to its property and the required packet delivery probability, but this scheme does not considers any attack.

XufeiMao,ShaojieTang,XiahuaXu,HuadongMa[3] focused on opportunistic method to minimize energy consumption by all nodes but this method does not consider any attack at routing level. Opportunistic routing is based on the use of broadcast transmission to expand the potential forwarders that can assist in the retransmission of data packets. By this method nodes in the forwarder list are prioritized and the lower priority forwarder will discard the packet if the packet has been forwarded by a higher priority forwarder. Adversaries who use a small number of packets i.e. protocol compliant in which intelligent packetdropping strategies can degrade performance of TCP streams traversing those nodes. Adversaries are also protocol-compliant in the sense that they use well-formed routing protocol messages. They either produce messages when honest nodes would not used, or send packets with protocol headers different from what an honest node would produce in the same situation.

GergelyAcs, LeventeButtyan and IstvanVajda[4]proposed a Provably Secure On-Demand Source Routing In Mobile Ad Hoc Networks. Routing is one of the most basic networking functions in mobile ad hoc networks. Hence, an adversary can easily paralyze the operation of the network by attacking the routing protocol. These attacks clearly demonstrate that flaws can be very subtle, and therefore, hard to discover by informal reasoning. It proposes a mathematical framework in which security can be

precisely defined, and routing protocols for mobile ad hoc networks can be analyzed rigorously.Regarding the capabilities of the adversary, it can mount active attacks i.e., it can eavesdrop, modify, delete, insert, and replay messages from corrupted nodes that have the same communication capabilities as the nodes of the honest participants in the network .A problem with the protocol, and often, one can construct an attack by looking at where the proof failed. Many researchers, and several "secure" routing protocols have been proposed for ad hoc networks. However, the securities of those protocols have been analyzed either by informal means only, or with formal methods that have never been intended for the analysis of this kind of protocols. These attacks clearly demonstrate that flaws can be very subtle, and therefore, hard to discover by informal reasoning. Consequently, it is also difficult to gain sufficient assurances that a protocol is free of flaws. The approach of verifying the protocol for a few numbers of specific configurations can never be exhaustive, and thus, it is far from being satisfactory as a method for security analysis.

Tuomas Aura, PekkaNikander, JussipekkaLeiwo[5] proposed dos-Resistant Authentication With Client Puzzles.Public-key authentication does not completely protect against the attacks because the authentication protocols often leave ways for an unauthenticated client to consume a servers memory space and computational resources by initiating a large number of protocol runs and inducing the server to perform expensive cryptographic computations. A solution to such threats is to authenticate the client before the server commits any resources to it. The authentication, however, creates new opportunities for DOS attacks because authentication protocols usually require the server to store session-specific state data, such as nonce, and to compute expensive public-key operations. It shows how stateless authentication protocols and the client puzzles of Juels and Brainard can be used to prevent such attacks. The protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

3.PROBLEM DEFINITION

Wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks due to their ad-hoc organization, and a great deal of research has been done to enhance survivability. Energy is the most precious resource for sensor networks The vampire attack is a genuine issue in remote sensor systems.Vampire attack can be defined as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. Vampire attack happens in the network in the sense, any of the nodes in the network which is affected or infected and this nodes behavior is abruptly changing for the network behavior, this kind of nodes are called malicious nodes. If any malicious nodes are present in the network then the energy that have been used by each and every nodes will increases drastically. Energy usage is measured for the minimum number of packets required to deliver a single message. Here two variations of vampire attacks are described.In the first type of attack, an adversary or malicious node composes packets with purposely introduced routing loops.It is called the routing loop attack and it targets source routing protocols by exploiting the limited verification of message headers forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

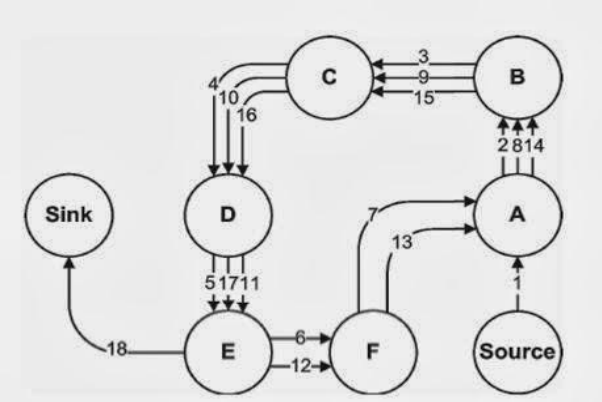

Fig -3.1: Routing Loop Attack

Figure3.1 shows routing loop attack in which normal path is source->A->B->C->D->E->sink. After attack introduces loops in a route,then route becomes source->A->B>C->D->E->F->A->B->C->D->E->F->A->B->C->D->E->sink.Energy required by the node A, B,C, D, E is doublethe normal energy.

In the second type of attack, also targeting source routing, an adversary or a malicious node constructs artificially long routes while traversing every node in the network.It is called the stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. This is one of the major problem of the network where energy consumption of each and every nodes in the network will be increasing.

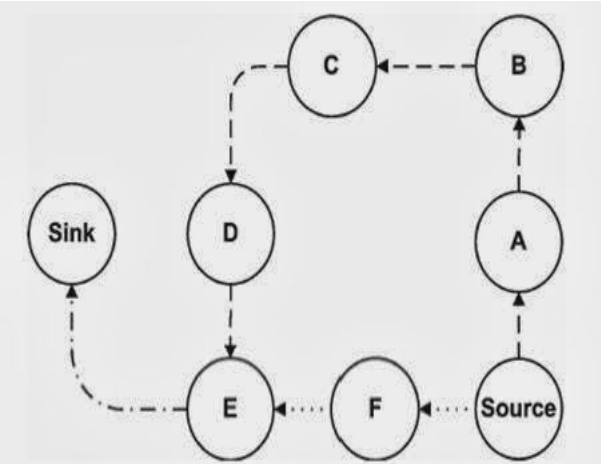

Fig -3.2: Stretch Attack

Figure 3.2shows normal route and alsoroute caused by attack. Dotted lines shows normal route path (source->F->E->sink) and other line shows infected route path (source->A->B->C->D->E->sink).

The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. The main characteristics of this type of attackers are its not easily identified if it attacked or affected the network, it will take some long time to identify and make ensure that it presented in the network.

4.EXISTING SYSTEM

In the existing system a methodology is proposed to increase the energy efficiency of the network and protection from vampire attack. For increasing energy efficiency of the network, an FDPM(Flexible Deterministic Packet Marking) algorithm is used. The FDPM algorithm is proposed to address the vampireattack.FDPM algorithm reduces the energy usage of the networks by avoiding vampire attacks and thus increases the network life time.The algorithm is used for secure and reliable data transfer.It does secure forwarding of packet to destination posture of the node.

4.1 METHODOLOGY

In this work,a layered approach is used to solve the problem with the vampire attacks.Malicious packets (vampire packets) are monitored both in network layer and in the application layer. The checking performed in network layer helps to point out the vampire packets from the network and the checking done in the application layer helps to find out the vampires inside the running processes (ie, inside the node). Whenever an incoming packet is detected as a vampire then the packet will not be forwarded and it will be discarded. Whenever a vampire is detected inside the node thenwe can simply eliminate it.The system concentrates on a secure data transmission from the adversary nodes in the sensor network. In order to build a secure network, the network should be an extinct to adversary nodes.Therefore an energy constraint anomaly detection method is used to detect the malicious nodes from the network. During the deployment of the network almost all nodes have the same energy. The energy or power of nodes is used for transmission or forwarding of data packets. Thus there will be a small variation in energy level of nodes. In the presence of vampire attack, it causes more energy to be consumed than a network with normal node does for the same processing and forwarding. Thus it makes the energy of whole network very much low.Energy constrained anomaly detection is based on the concept of energy level. It works on the fact that the malicious nodes will have abnormally high energy than legitimate nodes.A technique called Entropy Estimation is proposed to provide a flexible and fast approach to estimate the baseline distribution. Entropy estimation is a framework for obtaining a parametric probability distribution model from the training data and a set of constraints on the model. Entropy estimation produces a model with the most 'uniform' distribution among all the distributions satisfying the given constraints.

A mathematical metric of the uniformity of a distribution P is its entropy:

$$H(p) = \sum_{\omega \epsilon \Omega} P(\omega) log p(\omega)$$

Let Ω be the set of packet classes and given a sequence of packets S = (x_1,x_2…x_n) as the training data, the empirical distribution $\tilde{P}$ over in this training data is

$$\tilde{P}(\omega) = \frac{\sum 1(xi \, \epsilon \, \omega)}{n}$$

where 1(X) is an indicator function that takes value 1 if X is true and 0 otherwise.The nodes whose energy level has exceeded threshold value other than normal nodes is considered to be malicious nodes and will undergoes a vampire attack. Thus the energy of all the nodes are calculated and the node with abnormally high energy is detected as malicious node. Maximum nodes have an average energy level in certain range,and due to the nature of vampire nodes they have an abnormal energy level.By the proposed anomaly detection method we can calculate the threshold value and energy level of all nodes after every data iteration process. The proposed energy level constraint anomaly detection method efficiently detects the malicious nodes from the network, and by detecting those affected nodes we can form the secure network with authenticated data transmission. After the malicious nodes are detected,it will be represented graphically. Malicious nodes will be represented in green color and normal nodes will be represented in blue color. It will also give options to display the port scanning details.

Algorithm

```
If(load of router R>threshold Lmax)
  do not mark any packets
  turn on congestion control mechanisms
else if(load of router R>threshold Lmin)
  turn on flow based marking at R,edge interface A,
in network N
  for each incoming packet p
    check npkts with same destination address of p from T
    if(npkts==0,means no such flow in T)
      add a new entry in T,set its npkts=1
    else
npkts++
    insert packet p into Q
    calculate marking probability Pa
    with probability Pa mark the packet
(encoding procedure)
    if Q is full
dequeue
else
mark all the packets at R,edge interface A,in network N
```

4.2ADVANTAGES

- Protection from vampire attacks
- Secure level is high
- Boost up the battery power
- Save adhoc wireless nodes from power drainage due to vampire attacks
- Ease of use

4.3DISADVANTAGES

- The method does not provide a control on the respective IPs.

5.PROPOSED SYSTEM

In the proposed system,arule based classification is proposed to identify policy anomalies.It generates a new ruleset and on the basis of a new ruleset, it does rule based classification so that we can have a control on the respective IPs and thus make the network live.The proposed method aims in anomaly detection through firewall policies.Here we decide which packets to allow to go through or to drop based on a set of “rules” defined by the administrator.It comprisesa list of ordered filtering rules that define the actions performed on matching packets. A rule comprises of network field such as protocol type, source IP address,destination IP address, source port and destination port, and an action field.Actions are either to accept, which passes the packet into or from the secure network, or to deny, which causes the packet to be discarded. If the packet header information matches all the network fields of this rule,then the corresponding packets are retrieved and if there occurs any redundancy in the packet or if a particular node is considered as malicious then immediately a warning message appears.

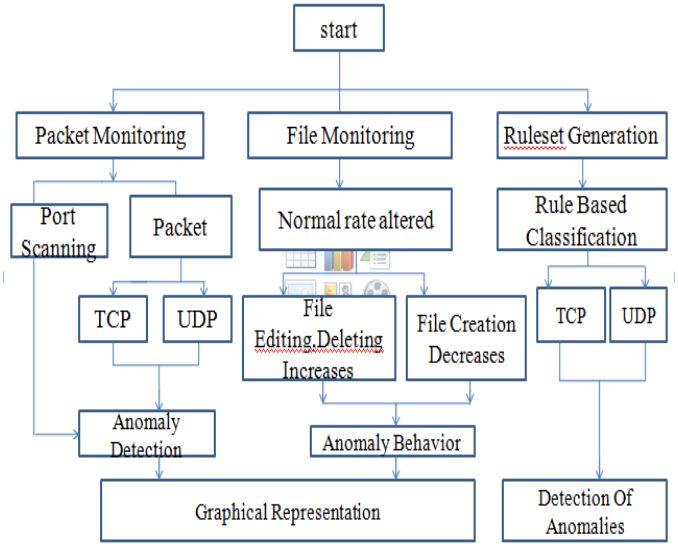

Fig -5.1: Proposed System Architecture

Algorithm

1: **Input:**
2: U:the universal character set;
3: M:the number of independent character sets;
4: W(c):the weight of character c;
5: **Output:**
6: independent character sets $U_{1,\ldots\ldots,}U_{M;}$
7: residual character set $U_{M+1;}$
8: U_k:=$\emptyset(k = 1, \ldots., M + 1);$
9: $W(U_k)$:=0(k=1,....M);initialize the weight of set U_k
10: Sort U in decreasing order of the character weight.
11: If U is empty,return (U_k)(k=1,.....M+1));
12: From U select the character c with the largest weight
13: Select the set U' with the smallest weight among sets U_1,.....U_M whose characters are all independent of c.If there is more than one such set,select the first one.
If no such set is found,put c into set U_{M+1},
remove c from set U and go to step 11.
14: c into set U';remove c from set U;W(U')+=W(c);
Go to step 11.

5.1 MODULE DESCRIPTION

Port Scanning system

In the port scanning module, the main aim is to check the status of the ports. After scanning the IP address and port number, system process details can be retrieved. The port scanning module identifies open ports and services available on a network host. Port scan details can be retrieved by continuously monitoring all open ports in the node

Packet monitoring System

In the packet monitoring module, in order to detect vampires from the network, an ad-hoc sensor network is needed to create. The vampire detection system can be installed in a node as an administrative tool. The IP addresses of all the nodes in the network are needed to retrieve.Analysis of TCP,UDP,DNS and ICMP headers will be done for packet monitoring. After monitoring all the incoming packets,the packets will pass through the anomaly detection system. On the basis of anomaly behavior, if an anomaly is present, an attack will be detected and the corresponding IP address of the malicious packet can be retrieved.

File monitoring system

All the activities such as creation, editing and deletion of the files are monitored to find application layer vampires. Normally if an anomaly is present, then the normal rate of these processes will be altered. The file editing and deleting rate will increase drastically and file creation rate will decrease.Consumption of memory will also increase in an abnormal fashion.Here a File SystemWatchercomponent is used to monitor a file system and react when changes to the directories or files it contains occur. This makes it possible for us to quickly and easily launch business processes when certain files or directories are created, modified, or deleted. For example, suppose you and a group of coworkers are collaborating on a document that is stored on a shared directory on your server. Using an instance of the FileSystemWatcher component, you can program your application to watch for changes to the contents of that shared directory. We can configure the component to watch either an entire directory and its contents or a specific file or set of files within a given directory. The FileSystemWatcher component raises an event whenever a file or subdirectory within the specified root directory is created, deleted, renamed, or changed in some other way. The types of changes that the component monitors include changes in the file's or subdirectory's attributes, size, last write time, last access time, and security settings.

Graphical analysis of energy consumption

In this module,nodes consuming more energy will be shown in green color and the normal nodes will be shown in blue color.Nodes consuming more energy will be blacklisted and its IP address will be made off, so that others will gain more energy.

Ruleset Generation

According to a specific protocol,we will be creating our own set of rules so that we can have a control on the respective IPs.It focusses on creating our own set of rules to identify policy anomalies.A rule can be defined as a set of criteria and an action to perform when a packet matches the criteria.The criteria of a rule consist of rule number,sourceIPaddress,DestinationIPaddress,Action,Protocol,Source Port,Destination Port. Therefore a complete rule may be defined by the ordered tuple <Rule Number, Protocol, Source IP, Source port, Destination IP, Destination port, Action>.The rules are in the form of a criteria and an action to take place if any packet matches the criteria.Actions are usually allow and deny.When a specific rule is to be created,an add rule button is to be clicked.Similarly when a specific rule is to be deleted,the delete rule button is to be clicked.

Table -5.1.1: Ruleset Generation

Rule	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
r_1	UDP	10.1.2.*	*	172.32.1.*	53	deny
r_2	UDP	10.1.*.*	*	172.32.1.*	53	deny
r_3	TCP	10.1.*.*	*	192.168.*.*	25	allow
r_4	TCP	10.1.1.*	*	192.168.1.*	25	deny
r_5	*	10.1.1.*	*	*	*	allow

Rulebased Classification

We implement the Security policy of the network by deciding which packets to let through based on a specific set of rules. A policy consist of a sequence of rules that defines the actions performed on packets that satisfy certain conditions.The rules are specified in the form of a <condition,action>.A condition in a rule is composed of a set of fields to identify certain type of packets matched by this rule.If any duplication in the packet arrives or if a particular IP is considered as malicious,immediately a warning message will occur.

6.COMPARISON AND ANALYSIS

Table -6.1: Comparison of existing and proposed method

	Existing Method	Proposed method (Rule Based)
Trace Length (seconds)	3600	3600
Number of packets	874613	1074132
Avg packet rate(per second)	242.9	298.3
TCP Packets	303142	403433
UDP Packets	571471	670699
Anomaly Detection rate	147	320

When number of packet increases the rate of anomaly detection also increases.

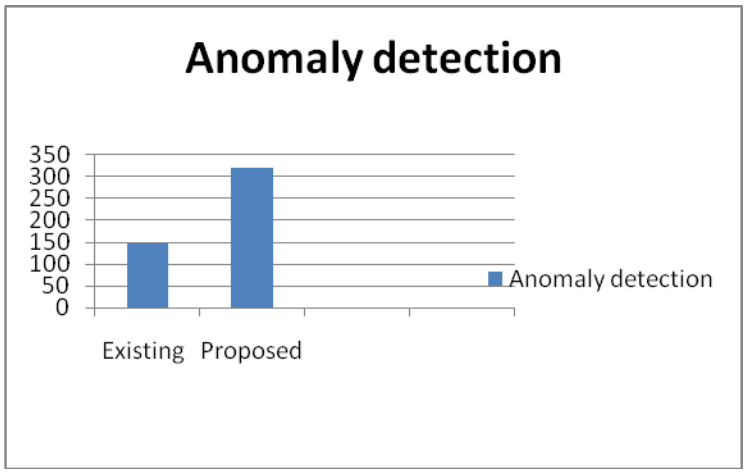

Chart -1: Analysis Of Existing And Proposed System

7.CONCLUSION

In this paper a detection and control method is introduced for the vampire attacks.The proposed methodology can be implemented as four phases, network layer vampire detection, Applicationlayer vampire detection, Vampire handling and entropy and port scan details. By using all these concepts the system is made more secure against the vampire attacks. Methods are there to detect the

vampires from the network and inside the node. By using FDPMAlgorithm the packets can be safely forwarded in a network. This scheme provides high level of security against the vampire attacks.Also by rule based classification detection of anomalies is done in a better manner.

REFERENCES

[1] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols"(2009).

[2]FatmaBouabdullah, NizarBouabdullah,RaoufBouabdullah "Cross-layer Design for Energy Conservation in Wireless Sensor Networks", IEEE GLOBECOM 2008,New Orleans,USA,December 2008.

[3] XufeiMao,Shaojie Tang, XiahuaXu, "Energy efficient Oppurtunistic Routing in Wireless Sensor Networks", IEEE transactions on parallel and distributed systems, VOL. 12, NO. 2, February 2011

[4] GergelyAcs, LeventeButtyan, and IstvanVajda, Provably secure ondemand source routing in mobile ad hoc networks, IEEE Transactionson Mobile Computing 05 (2006), no. 11

[5] NTuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[6] ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

BIOGRAPHIES

BharathyVijayan received B.Tech degree from M.G College Of Engineering,Kerala and currently pursuing M.Tech in Computer Science & Engineering at LourdeMatha College of Science &Technology,Kerala.Her areas of interest include Mobile Computing & Data mining.

