Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.100 – 109

RESEARCH ARTICLE

Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network

V.Sharmila[1], Mr. K. MuthuRamalingam[2]

[1]School of Computer Science, Engineering and Applications, Bharathidasan University, Trichy, India
[2]School of Computer Science, Engineering and Applications, Bharathidasan University, Trichy, India
[1] vsharmila1991@gmail.com, [2] jmcmuthu@yahoo.co.in

Abstract— one of the most complicated attacks in wireless sensor network is energy depletion attack. In which vampire attack and Distributed Denial of Service (DDOS) attack were leading. In this paper using a newly proposed Enhanced Ad Hoc on-Demand Vector (ENAODV) routing protocol, the link break at distant node is repaired with alternate path selection of shortest route in secure manner. The Adaptive Traffic Coalescing (ATC) scheme and Adaptive Power Aware Multicasting (APAM) Algorithm are used to detect a DDOS attack and an incoming traffic monitoring at least energy consuming path selection at network nodes. As a result of simulation, the performance given is related to the energy level and its packet delivery ratio in respect to time consumed.

Keywords— Wireless Sensor Network, Vampire attack, Adaptive power multicast, DDOS, ENAODV, MANET

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Ad Hoc Networks have the attributes such as wireless connection, continuously changing topology, distributed operation and easy of deployment. Each node operates not only on end system, but also as a router to forward packets. Routing in Ad Hoc Networks has been a challenging task ever since the wireless networks came into existence.

Moreover, consuming less energy and increasing the life time of the wireless sensor nodes are the main objectives in designing the WSN, because of the limitation of the power resources and the difficulties of replacing the batteries of the wireless sensor nodes. However, designing an efficient routing protocol for WSNs is a greater challenge than for any other computer network. An essential part of developing WSNs is being energy aware by reducing the power consumption because of the power limitation. The following are some of the energy depletion attacks that cause the nodes to use more energy and drain its whole power.

A. Denial Of Service Attack

A denial-of-service attack DoS attack or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

B. Vampire Attacks

Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic and beacon routing. Neither do these attacks 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.

C. *Malicious Discovery Attack*

Another attack on all previously mentioned routing protocols including statefull and stateless is spurious route discovery. In most protocols, every node will forward route discovery packets and sometimes route responses as well, meaning it is possible to initiate a flood by sending a single message. Systems that perform as-needed route discovery are particularly vulnerable, since nodes may legitimately initiate discovery at any time, not just during a topology change. A malicious node has a number of ways to induce a perceived topology change: it may simply falsely claim that a link is down, or claim a new link to a nonexistent node.

The objective of this paper is to illustrate the means of vampire attack and DDOS attack and also about the link break occurrence at distant node and blocking the attacker node. The remainder of the paper is organized as follows. Section 2 describes some of the works related to routing in ad hoc networks. In section 3, the proposed new technique is presented. In section 4, the simulation environment, parameters, and results are obtained for the WSN. Finally, we conclude the paper in section 5.

II. RELATED WORKS

Provably Secure On-Demand Source Routing In Mobile Ad Hoc Networks

[3]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. In framework is tailored for on-demand source routing protocols, but the general principles are applicable to other types of protocols too. 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

Drawbacks

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.

Fast Implementations of AES on Various platforms

[5]Target platforms are 8-bit AVR microcontrollers, NVIDIA graphics processing units and the Cell broadband engine. The new AVR implementation requires 124.6 and 181.3 cycles per byte for encryption and decryption with a code size of less than two kilobyte. As the outcome of a public competition, Rijndael was announced as the Advanced Encryption Standard by the US National Institute of Standards and Technology. The byte-sliced implementation for the synergistic processing elements of the Cell architecture achieves speed of 11.7 and 14.4 cycles per byte for encryption and decryption. The other target platforms, the Cell and the GPU, are chosen because of their ability to process many streams simultaneously, using single instruction, multiple data and single instruction, multiple threads techniques respectively.

Drawbacks

That although direct addressing can access the whole data space, indirect addressing with displacement is limited to 63 address locations from only one of the pointer registers, and this restriction may require the implementer to use techniques such as double-jumping. Another limitation is that only the Z register may be used for addressing ash memory, e.g., for AES S-box lookups, and in some AVR devices this is not possible at all.

Denial of Service Resilience In Ad Hoc Networks

[2]Significant progress has been made towards making ad hoc networks secure and DoS resilient. There remains an indefinite "arms race" in system and protocol design: attackers or researchers anticipating the moves of attackers will continually introduce increasingly sophisticated attacks, and protocol designers will continually design protocol mechanisms designed to thwart the new attacks. It design and study DoS attacks in order to assess the damage that difficult to detect attackers can cause. One perhaps surprising result is that such DoS attacks can increase the capacity of ad hoc networks, as they starve multi-hop flows and only allow one-hop communication, a capacity-maximizing, yet clearly undesirable situation.

Drawbacks

However, no TCP variant is robust to malicious and persistent reordering as employed by the JF disordering attack. The second JF mechanism is periodic dropping according to a maliciously chosen period. Intuitively, if a system has no mobility and infinite route lifetimes JF will have little effect as nodes will eventually discover routes without JF if such routes exist. However, as mobility increases, the route lifetime shortens and the effects of JF become increasingly pronounced as the time spent uselessly transmitting on JF paths and re-establishing routes becomes an increasing fraction of a flow's lifetime. Thus, an analytical and experimental relationship that characterizes the impact of these timescales on flow good put.

New AES Software Speed Record

[6]The new speed records for AES software, taking advantage of architecture-dependent reduction of instructions used to compute AES and micro architecture-dependent reduction of cycles used for those instructions .Almost all of the specific techniques it use are well known. The main novelty lies in the analysis and combination of these techniques, producing surprisingly high speeds for AES. There are also, in the literature, many different ways to benchmark AES software. This variability interferes with comparisons.

Drawbacks

First, some applications en- crypt long streams and do not mind padding to 2048-byte boundaries; second, some applications will use bit slicing on both client and server and can thus eliminate the costs of transposition; third, bit sliced implementations are inherently immune to the cache-timing attacks.

DOS-Resistant Authentication with Client Puzzles

[4]Public-key authentication does not completely protect against the attacks because the authentication protocols often leave ways for an unauthenticated client to consume a server's 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.

Drawbacks

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.

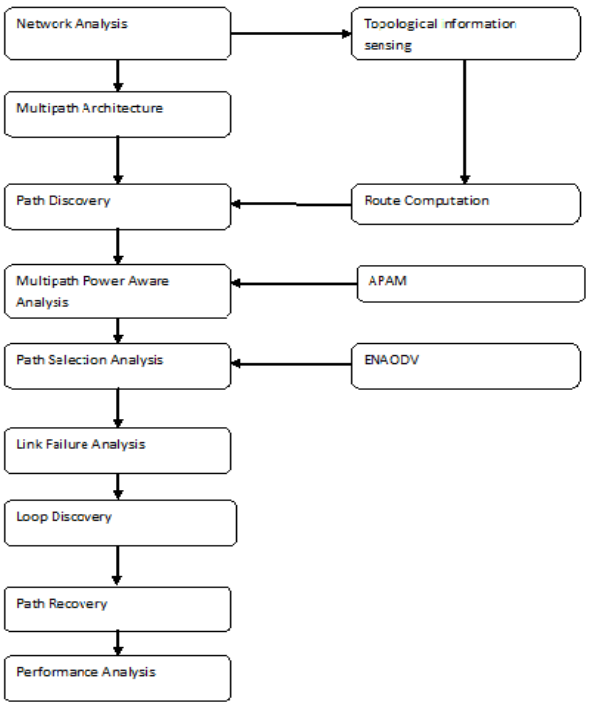
III. PROPOSED WORK

The major reason for this continuous network topology changes is because of high degree node mobility. A number of protocols have been developed to accomplish this task. In this proposed approach, we address the problem of vampire attack and DDOS attack that may cause energy depletion of the network nodes. And further we have used the technique to eliminate/block the vampire attack with efficient routing Ad Hoc Networks.

The energy of the nodes is the major area of concerned for the research to be carried on in this field. One of the methods suggested was Adaptive Power Aware Multicast Algorithm (APAM). The energy factor of the nodes is taken as the major concern in this algorithm.

In order to detect the Vampire attacks and DDOS attacks a newly proposed routing protocol named Enhanced Ad Hoc On-Demand Distance Vector (ENAODV) has been suggested that selects the path from source to destination on basis of the path that consumes the least energy and of shortest path. The path selected for this transmission is the best selected path for the particular type of nodes. And also it is capable of repairing the link break at distant node with alternate path of shortest route in secure manner.

Flow diagram:



Once the attacking packets have been blocked and the victim is recovering, it's time to trace the command and control infrastructure behind the DDOS-attacking. DDOS attacks cannot be detected effectively by traditional methods in time, a DDOS attack detecting algorithm based on the relation of characteristic parameters is researched according to the analysis of the essential characteristic of DDOS. The scheme can detect DDOS attack traffic in its early stages when the attacking packet's attribute value has no distinct features. It can differentiate DDOS from normal flash crowd traffic.

The Scheme Adaptive Traffic Coalescing (ATC) monitors the incoming traffic and can detect DDOS attack traffic in its early stages when the attacking packet's attribute value has no distinct features. It can differentiate DDOS from normal flash crowd traffic. The feature ATC scheme effectively reduces platform wake events, and enables the platform to enter and stay in the low-power state longer for energy efficiency.

To enhance the performance robustness of the system, under base station failure events, it extends the basic algorithm by introducing an opportunistic relay aided multicasting operation. Under the extended multicasting protocol, in addition to using base stations to multicast messages to nodes that are located closer to them, mobile stations can be elected to relay multicast messages that they have received directly from their base stations to peripheral nodes in their neighbourhood.

It shows that this extended adaptive power and rate multicasting scheduling algorithm is effective in adapting to a failure of a base station node, limiting the performance degradation that is incurred. For an illustrative scenario, the extended relay aided scheme is noted to yield a throughput rate that is higher than that attained by a scheme that doesn't employ relay nodes by about 20%, while consuming less energy resources.

ENhanced Ad Hoc On-Demand Distance Vector (ENAODV) routing protocol

An intermediate node are usually nearer to the destination than the source node, the intermediate nodes on the route are comparatively more suitable in comparison to the source node to broadcast the RREQ message in order to repair or find an alternate route to the destination.

Based on this idea, adopted the intermediate nodes that were en-route to repair the broken route to the destination. The standard version AODV protocol uses three types of packets for communication via RREQ (Route Request), RREP (Route Reply), and RERR (Route Error).

In addition to these three communication packets we have introduced three more packets via R_R (Route Repairing), RR_OK (Route Repair OK), and RR_F (Route Repair Failure).

If data is flowing from S to D via nodes A, B, C and a link break is detected by the intermediate node B, B does not send a RERR to the source of the data S. Instead, it sends a Route Repairing (R_R) message back to the Pre-hop node A. After sending R_R to A, B tends to broadcast RREQ to repair the break route.

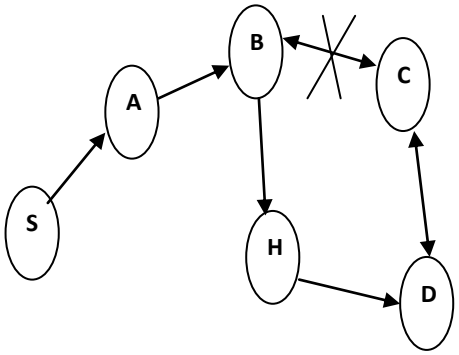


Figure 1: Depicting route invalidation

If B cannot repair the route in certain amount of time, it sends back a Route Repair Fail (RR_F) message to A. And at same time B sends the data packages, which store in the cache, back to A. Otherwise, once B repairs the route in time, if sends back a Route Repair OK (RR_OK) message to A which has received a R_R message.

Once node A receives a R_R message, it caches the data packages sent to the destination. If A, which is not the source node of the data has received a RR_F message from the break node, A sends a R_R message back to the Pre-hop of itself and continues the same procedure. On the contrary, if node A receives a RR_OK message which means the break link is repaired by B, it sends all waiting data packages stored in the cache.

PSEUDOCODE:

Step 1: If ((Node B identifies link error) AND (node is an intermediate Node))

{

B caches the data packets arriving;

B broadcast RREQ message;

B initiates a timer;

B sends R_R message to its pre-hop node;

}

Step 2: Else if ((Node B has already broadcasted RREQ message) AND (timer is expired) AND (B is an intermediate node))

B sends RR_F back to its pre-hop node;

B sends cached data back to pre-hop node;

}

Step 3: Else if ((Node B has sent R_R message to its Pre-hop) AND (B successfully repairs the link) AND (B is an intermediate node))

{

B forwards cached data packets to the next hop;

B sends RR_OK message to its pre-hop node;

}

STEP BY STEP PROCEDURE

Step1: start establishing the network

Step2: Analyse the network

Step3: Process of Multipath Routing

Step4: ATC checks for the presence of attacks like jamming, vampire, ddos

Step5: Include the ENAODV process regard on-demand analysis of distance

Step6: Then the data packets are forwarded to next node/hop

Step7: Adaptive Power Aware Multicasting is done to save energy compared to analysis of time means

Step8: Acknowledgement is send to source after receiving the data packs

Step9: End

IV. SIMULATION RESULT

The simulation environment is implemented in the NS-2, a network simulator that provides support for simulating wireless networks. NS-2 [8] is written using C++ language and uses the Object Oriented Tool Command Language (OTCL) [9]. It is an extension of the Tool Command Language (TCL).

Detection of Vampire Attack

We have evaluated both the carousel and stretch attack. A randomly generated 10 node topology for carousel attack and 16 node topology for stretch attack is taken. A single randomly selected malicious AODV agent, using ns2 network simulator is evaluated. The total energy set is 10J. For the stretch attack the energy consumed by the system is 4.37960 J and for the carousel attack the power consumption is 4.625225 J.

The energy calculated is given by the formula:

$$Energy\ Consumed = \frac{EI-EF}{EI}$$

EI - Initial Energy
EF - Final Energy

The initial value in both the cases is assumed to be 10J. The simulation is done for 10ms. The data is transmission begins at 5ms and ends at 10ms.

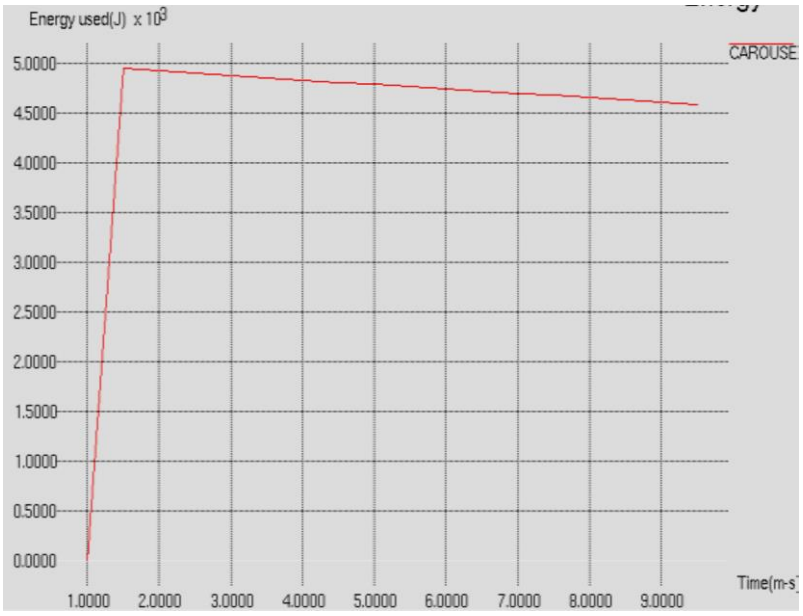


Figure2 Energy consumption in carousel attack

Figure2 shows the energy consumption during a carousel attack where the x axis is taken as the Time (ms) and the y axis is taken as the Energy (J) used that is done by the formula mentioned earlier. Energy consumption is 4.37960J for every 10J. Since the initial energy is 10J the peak rises above and then gradually decreases with the transmission of data and in the presence of carousel attack.

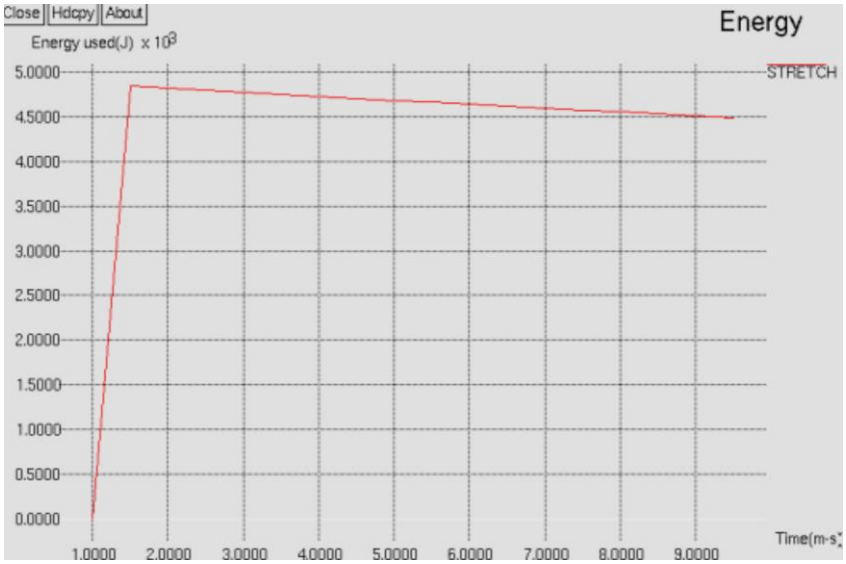


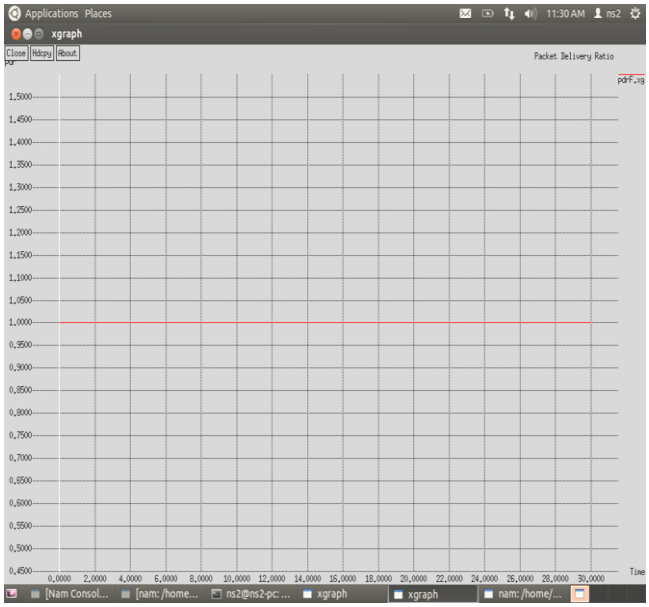
Figure3 Energy consumption in stretch attack

Figure3 shows the energy consumption in stretch attack where the x axis is taken as the Time (ms) and the y axis is taken as the Energy (J) used. The energy consumption in this case is 4.625225J for every 10 J. This value increases with the increase in number of nodes.

The packet delivery ratio is calculated by means of using the formula in relation to time :

$$Packet\ Delivery\ Ratio = \frac{No.of\ Packet\ Recieved}{no.of\ Packet\ send}$$

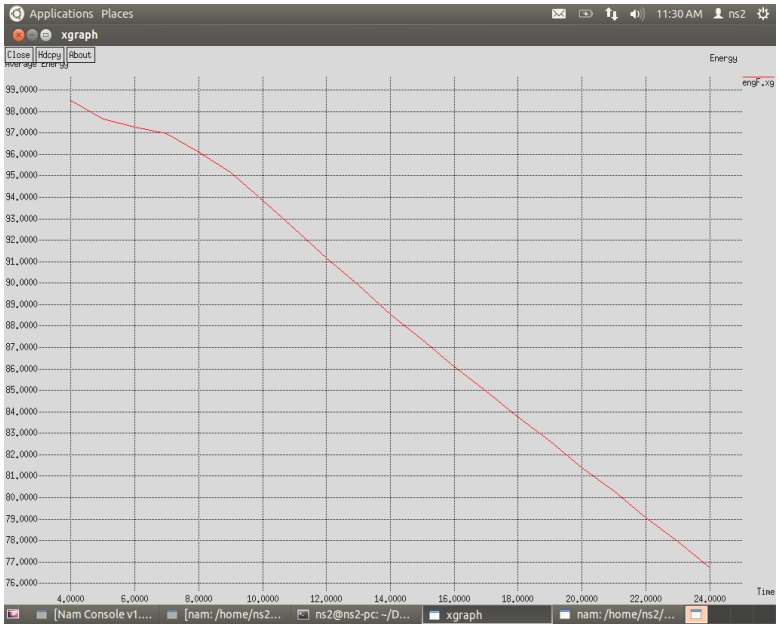
The simulation result regard the packet delivery ratio is shown below:



Energy Level:

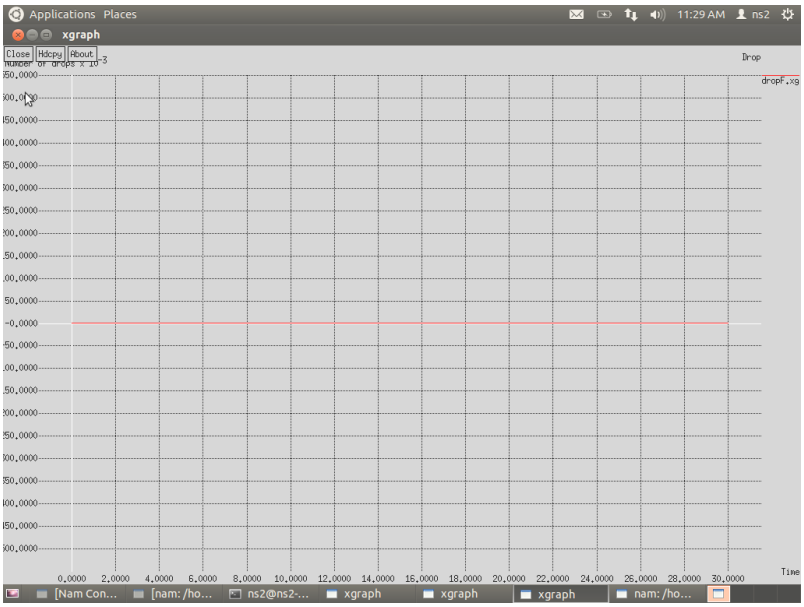
The energy level for the simulation result stated here is calculated regarding the following formula in relation to time.

$$Energy\ Level = Recieved\ packet + signal\ strength + power\ management$$



The time is calculated by means of:

$$Time = No.of\ packets + Recieved\ Packet + Loss + Position$$



V. CONCLUSION

In this paper the attacks of energy depletion are detected and blocked by means of using the effective routing protocol ENhanced Ad Hoc on-demand Vector routing protocol (ENAODV) and save the power by Adaptive power aware Multicasting algorithm. The DDOS attacks are prevented by means of the scheme Adaptive traffic coalescing (ATC). Thus the securing of network nodes energy is carried out and finding alternate path for route link broken is done. The simulation result proves the improvement in the energy consumed and packet delivery ratio in relation to time.

REFERENCES

[1]. Eugene Y. Vasserman and Nicholas Hopper, In 2013, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks.

[2]. I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[3]. G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[4]. T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int"l Workshop Security Protocols, 2001.

[5]. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.

[6]. D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int"l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[7]. I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ, 1999.

[8] "The Network Simulator- ns-2" http://www.isi.edu/nsnam/ns.2012.

[9] V. Vijaya Raja, R. Rani Hemamalini, and A. Jose Anand, "Multi Agent System Based Upstream Congestion Control in Wireless Sensor Network", 2011

