Defense against Damage Bounds for Topology Discovery and Packet Forwarding phase in Wireless Ad Hoc Sensor Networks

E. GAYATHRI, Dr. N. GEETHANJALI

Abstract

Wireless adhoc networks are widely used networks as they provide convenient solutions to sensing problems in both civilian and military domains. The nodes in Wireless Sensor Networks (WSNs) are to be protected from adversaries as they are vulnerable to various attacks. Many protocols came into existence to secure communication in WSNs. However, there was less research found in the literature with respect to energy depletion attacks that reduce the quality and availability of network. Recently Vasserman and Hopper introduced a protocol named PLGPa that could provide satisfactory solution to special kind of energy depletion attacks named Vampire Attacks. Especially, they presented carousel and stretch attacks that could waste energy of source nodes and reduce the life of network. Their solution was incomplete as it could not safeguard the network in Topology Discovery Phase and Packet Forwarding Phase. Their protocol could not bound the damages caused by vampires in Topology discovery phase. In this paper, we extend their protocol in order to overcome the above stated problem . Our simulations show that the proposed approach is not vulnerable to vampire attacks.

Index Terms – Adhoc network, Damage bounds, Denial of service, Energy consumptions , Topology, Wireless network

1.INTRODUCTION

Adhoc Wireless Sensor Networks are widely used in the real world for sensing various environments. Very important aspect in this networks is the availability of nodes and the network in expected time. This is known as Availability of the network. The problems with availability are not tolerable in the real world applications. When the nodes in WSN are vulnerable to attacks like Denial of Service (DoS), they cannot promise to fulfill the availability feature which is very important expectation from such network. When the network availability itself is in stake, the purpose of such network is not served. Many schemes and protocols came into existence that could take care of DoS attacks in WSN. However, they could not solve long-term availability problems.

Unlike the wired networks that typically have fixed network topologies, each node in a wireless network can potentially change the network topology by adjusting its transmission range and/or selecting specific nodes to forward its messages, thus, controlling its set of neighbors. The primary goal of topology discovery phase is to control and to maintain network connectivity in wireless network, optimize network lifetime and throughput, and make it possible to design power-efficient routing. Not every connected subgraph of the unit disk graph plays the same important role in network designing. One of the perceptible requirements of topology control is to construct a subgraph such that the shortest path connecting any two nodes in the subgraph is not much longer than the shortest path connecting them in the original unit disk graph. This aspect of path quality is captured by the stretch factor of the subgraph.

There is a special kind of attack known as resource depletion attack which causes the nodes to lose energy faster and the availability of the network is jeopardized. These

ISSN: 2278 – 7798

attacks are different from other attacks pertaining to service denial and reduction of quality. They are named as vampire attacks as explored in [1]. Vampire attacks are classified into carousel attack and stretch attack. These two attacks have different approaches in which packets are led to unnecessary routes so as to ensure that the nodes' energy gets depleted over time. This is very potential risk in WSNs those cause availability problems. The packet forwarding phase in the solution [1] is not vulnerable to vampire attacks since it has backtracking capability. However, the protocol is not secure against vampire attacks in topology discovery phase.
Topology discovery. Discovery begins with a time limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key (from now on referred to as nodeID), signed by a trusted offline authority.

Our contributions in this paper are as follows.

- We improved the PLGPa protocol in such a way that it is not vulnerable to vampire attacks in topology discovery phase also. Moreover, it could bound damage on malicious discovery on the network in the presence of vampire attacks.

- We implemented the protocol and tested it with NS2 simulations that provide the proof of concept. The results reveal that the proposed solution is not vulnerable to vampire attacks both in packet forwarding phase and also topology discovery phase.

The remainder of the paper is structured as follows. Section 2 provides review of literature on energy depletion attacks and other related works. Section 3 proposed overview of the proposed system. Section 4 presents experiments and results while section 5 concludes the paper and section 6 provides recommendations for future work.

II. RELATED WORK

This section provides review of related works. Karp and Hung [2] presented a new routing protocol named as Stateless Greedy Perimeter Routing protocol for wireless networks. It is greedy in nature while making packet forwarding decisions by using local topology information. Karlof and Wagner [7] focused on security in wireless sensor networks. They worked out on threat models, selective forwarding,, sinkhole attacks, Sybil attacks, wormholes.. Hu et al. [8] presented various attacks against routing including denial of service attack. Their attacks and experiments are based on routing protocols. Their experiments revealed that source-routing helped to secure ad hoc networks. Kwok *et al*. [9] presented a methodology for halting anomalies in TCP sessions that are with facility known as weighted chocking. Doshi *et al*. [9] highlighted the significance of energy caching techniques for minimizing energy consumption in wireless ad hoc networks. Govindan and Anoop Reddy [10] studied on route stability and inter-domain analysis of Internet. Their findings include the lateral growth of Internet and degradation of route stability. Fonseca *et al*. [11] studied on beacon vector routing for scalable routing solutions in wireless sensor networks. Their approach forwards packets greedily and to the next hop for efficient and scalable network.

Kawahara *et al*. [12] focused on tate pairing on mobile phone for securing communications. Similar kind of research was carried out in [26] . Deng *et al*. [13] provided solution to prevent path-based DoS attacks. Their solution is light weight and it could tolerate packet losses in the context of bursty traffic. Kroller *et al.* [14] presented a framework that will help in topology extraction and recognition of deterministic boundary. Jhonson *et al*. [15] presented the dynamics of DSR protocol for efficient routing. Bos *et al*. [16] provide various forms of Advanced Encryption Standards for various target platforms. Deng *et al*. [17] presented an approach for routing which tolerates intrusions. This kind of solutions is good which can work even in the presence of attacks. Kuzmanovic and Knighty [18] focused on patterns of malicious traffic that is towards denial of service attacks on TCP with low packet rates. Luo and Chang [19] focused on pulsing DoS attacks and the solutions on it. Towards it they implemented a two-stage scheme that could detect such attacks. Goldberg *et al*. [20]

ISSN: 2278 – 7798

presented an approach for monitoring path-quality in the presence of attackers. Acs *et al*. [21] focused on routing protocols and identified flaws. The essence of their research was to ensure provably secure source routing. Guirguis *et al*. [22] focused on RoQ (Reduction of Quality) attacks and could quantify damage of such attacks. Hu *et al*. [23] designed and evaluated a protocol named Secure Efficient Ad Hoc Distance Vector Routing Protocol for securing communications in mobile ad hoc networks. Feldhofer *et al*. [24] explored AES algorithm for secure authentication mechanism in RFID systems. Douceur [25] focused on Sybil attacks that are related to multiple identities.

Vasserman and Hopper [1] focused on vampire attacks that drain life from nodes in ad hoc sensor networks. They focused on two kinds of attacks namely carousel attack and stretch attack. Their work is the first on the special kind of attacks known as vampire attacks. Vampire attack causes the network nodes to have unnecessary routing of packets in order to drain energy from nodes. This comprehensive study proves that such attacks could be made on any routing protocol. The limitation of their protocol is that it could not give guarantee in topology discovery phase while it is not vulnerable to vampire attacks in packet forwarding phase. In this paper we improve their protocol in order to overcome these issues.

III. PROPOSED SYSTEM

Vampire attacks where defined in [1] and the solution there is provided in the form of a protocol known as PLGPa. This protocol is not vulnerable to attacks in the forwarding phase as it can secure the network. However, it is not secure with respect to in the discovery phase. In this paper, we proposed an enhanced PLGPa algorithm where the limitations of [1] are overcome. By using a verifiable path history to every packet, it ensures that adversial influence is prevented besides taking the path to traverse at least one honest node. Another important aspect is that messages in the network are signed by originator. Only packet fields that go in different route only can be altered by adversary. In order to prevent this one-way signature chain is constructed. Hop count of packet is used in the signature which appears logically closer to the destination when compared with previous hop in the chain.

PLGPa includes path attestations, increasing the size of every packet, incurring penalties in terms of bandwidth use, and thus radio power. Adding extra packet verification requirements for intermediate nodes also increases processor utilization, requiring time, and additional power.

With respect to topology discovery phase, a certificate along with public key is broadcasted by each node. Each node in the network can have its group with size one and having virtual address zero. Then such group is merged with neighboring group which is smallest and group address is preceded by the own address of nodes. Thus each node is well aware of virtual address of other nodes, certificate of identity along with public key. In this context, routing discovery phase is optimized to minimize vulnerabilities that might cause attacks. We extended the PLGPa as per the intuition provided in [1] in order to bound damage from malicious discovery. Directional antennas can be used by malicious nodes and appear like group of size one thus become an attractive source for merging with other nodes. Requested group's id is used to compose merge requests and the receiving node causes the requests to flood to other members.

Theorem 1: In PLGPa algorithm, whenever the transmission of packet 'p' satisfies no-backtracking condition in the presence of an adversary controlling (m<n-3 nodes) and if 'p' checks the verifiable path history to every PLGP packet.

Proof:

Let us consider N be a network and n1,n2,…..n_k are indicates nodes of the network.

If p1,p2,…….p_l are indicates packets. PLGP arbitrary traces are there and 's' sends packet p to 'd'. Here's' indicates Source node,'d ' indicates Destination node, m indicates malicious and n indicates total number of nodes. The total number of nodes n=15. 'm' indicate as malicious and here m=10 and n-3 = 12. m<n-3 = 10<12 so it's as malicious controlling and attack the sending of packet. The purpose of

ISSN: 2278 – 7798

PLGPa forming groups and addressing of every node and it verifies path history of node. Whenever we transmitting packets to nodes, first creating routing tables at packet transmission time. Consider, at node n2. The routing table of a node n2 is n(2).whenever packet transmission occurs ,routing table should be updated so updated routing table of n(2) as a n (2)[rt_upd]. In case, some packets are not sent so should be treated as false packets. False packet routing table generated based on PLGPa. So Fp1, fp2,….fp_y are indicates as false packets. In the transmission process, energy levels are created to the correspond nodes and 'E_d' indicates the destination energy.

T**heorem2**: PLGPa is vulnerable to vampire attacks during the forwarding phase and satisfactory solution for topology discovery to recover the damages from malicious discovery.

Proof:

Let us consider N be a network and n1,n2,…..n_k indicates nodes of the network. If p1, p2,…….p_n indicates packets. HP1,HP2,HP3,……HP_n are the hop node of the network. Consider a node n3; The routing table of a node n3 is n(3).whenever packet transmission occurs ,routing table should be updated so updated routing table of n(3) as a n(3)[rt_upd].

rt_upd << next hpn(3)

The above condition is satisfied for vulnerability to vampire attacks during the forwarding phase. The above condition is not satisfied then routing table is updated. For instance, if node number is 3, n=3, next hop node is 5. Routing update value of n(3) is 2 (rt_upd = 2) 2<5 => condition is satisfied. If 'C' is a variable and node length is taken and corresponding variable length increased based on PLGPa, , then length = node length, otherwise length is zero.

The condition satisfied for malicious discovery phase.

Proposed Algorithm

Algorithm:

1. Start
2. Packets are transmitting from source to destination
3. Some packets are dropping
4. Attackers are started through network
5. Solve the verification of packet transmitting
6. Vampire attack holds the backtracking
7. PLGPa process started
8. If (every node verify the route path history)
9. Allow the connection to non-neighboring malicious node
10. Else packets are not verified and it goes to destination
11. If (node routing update is active)
12. False packet routing table<<next hop node
13. Else
14. If (node routing update is deactivate)
15. Update routing table<<next hop node
16. Else
17. Update routing table
18. If (energy ids of malicious node)
19. Update routing table<<destination id
20. PLGPa to bound damage from malicious discovery
21. Else packets are moving to neighboring nodes
22. End if
23. Else
24. Normal transmission of packets
25. Packets send to destination
26. End if
27. End

As the chain signatures described in PLGPa are very expensive to compute, they do not satisfy the strong unforgeability. The chain signatures require implementing a specialized secret key setup. To overcome the above disadvantages we enhance the PLGPa by using MVC scheme called MULTIVERIFIER SIGNATURES which are considered as strong signatures.

ISSN: 2278 – 7798

TIME COMPLEXITY:

The time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the string representing the input. The time complexity of an algorithm is commonly expressed using big 'O' notation, which excludes coefficients and lower order terms by using comparison sort and finds out the time complexity. In this project, comparison between plgp and plgpa is mentioned for execution time.

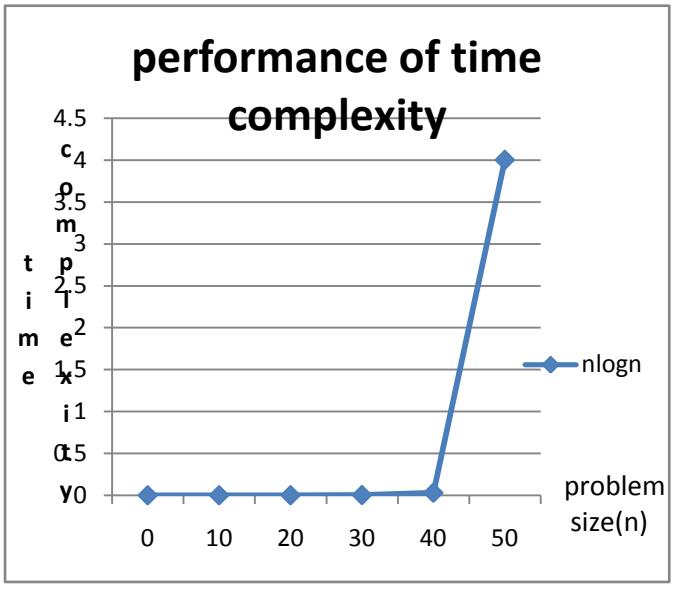
Problem size(n)	Time complexity(sec)
0	1µsec
10	15 µsec
20	200µsec
30	2.5µsec
40	30msec
50	4sec

complexity. In this project, comparison between plgp and plgpa is mentioned for execution time.

Consider d is depth and L is Length.

➔$d = (\log_2 n)$

➔$\sum_{L=0}^{d-1} 2(d-L)2^L$



Simulation and Results

A number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly generated topology of 50 nodes. Simulations are made using NS2 and showed the extended version of the PLGPa is not vulnerable to attacks both in forwarding phase and also in topology discovery phase besides having the ability to bound damage from malicious discovery.

PARAMETER	**SPECIFICATION**
Simulation tools used	NS2 Network Simulator (ns-2.35)
Simulation time	60 sec, 120 sec, 200 sec
Number of nodes	10,20,30,40,50
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	CBR [constant bit rate] [20]
Packet size	512bytes
Node mobility model	8packets/sec
Protocol	AODV
Number of runs	24

Table 1 – Simulation parameters

ISSN: 2278 – 7798

IV. RESULT ANALYSIS

Simulations are made to analyze the performance of the proposed protocol. The experiments are made in terms of number of malicious nodes versus detection performance, number of nodes versus end to end throughput, and energy consumption dynamics in the presence of attackers.

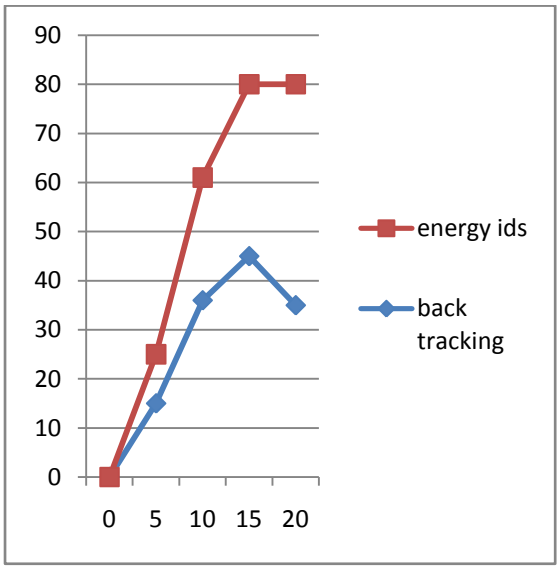
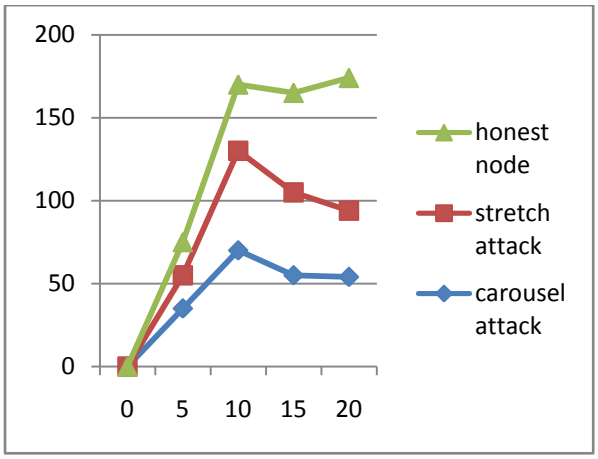


Figure 2 – Detection performance



As can be seen in Figure 2, it is evident that the graph shows vampire energy ids and vampire backtracking. Horizontal axis represents number of malicious nodes while the vertical axis represents detection performance.

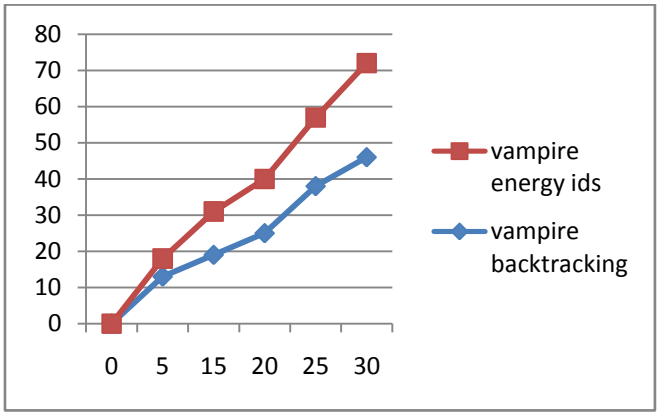


Figure 3 – Packet delivery performance analysis

As can be seen in Figure 3, it is evident that the graph shows performance analysis on packet delivery. Horizontal axis represents number of nodes while the vertical axis represents end to end throughput.

ISSN: 2278 – 7798

V. CONCLUSION

In this paper we studied the problems in topology discovery phase and packet forwarding phase However, our focus was on to enhance the PLGPa protocol implemented in [1]. The PLGPa was able to secure WSN against vampire attacks that deplete energy from nodes in the network causing the reduction of life of network besides lessening the availability of network. However, PLGPa could not provide satisfactory solution against vampire attacks in topology discovery phase. In this paper we presented an enhanced protocol that takes care of defense against vampire attacks in both packets forwarding phase and topology discovery phase. We made simulations using NS2 to demonstrate the proof of concept. The results revealed that our solution is robust against vampire attacks.

VI. FUTURE ENHANCEMENTS

A number of attacks in existing routing protocols by using a small number of weak adversaries have been explained, and measured their attack success on a randomly generated topology of 50 nodes. In future, the network energy expenditure during the forwarding phase can be decreased from 50 to 500 percent. Simulate how the energy is consumed by an single vampire to O(N). Handling vampires in mobile technology and factors of energy increase when multiple malicious nodes exist in network is left for future work.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper. (FEBRUARY 2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *IEEE*. 12 (2), p318-332.

[2] Brad Karp and H. T. Kung. (2000). GPSR: Greedy Perimeter Stateless Routing for Wireless Networks, p1-12.

[3] LAURA MARIE FEENEY. (2001). An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks. *IEEE*. 6 (-), p239–249.

[4] ANDREA J. GOLDSMITH and STEPHEN B. WICKER,. (August 2002). DESIGN CHALLENGES FOR ENERGY-CONSTRAINED AD HOC WIRELESS NETWORKS. *IEEE*. - (-), p1-21.

[5] Morteza Maleki, Karthik Dantu, and Massoud Pedram. (2002). Power-aware Source Routing Protocol for Mobile Ad Hoc Networks. -. - (-), p1-4.

[6] David Hwang Bo-Cheng Lai Patrick Schaumont Kazuo Sakiyama Yi Fan Shenglin Yang Alireza Hodjat Ingrid Verbauwhede. (2003). Design Flow for HW / SW Acceleration Transparency in the ThumbPod Secure Embedded System. -. 2 (6), p60-65.

[7] Chris Karlof and , David Wagner. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. -. 1 (-), p293–315

[8] YIH-CHUN HU and ADRIAN PERRIG , DAVID B. JOHNSON. (2005). Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. -. 11 (-), p21–38,

[9] Yu-Kwong Kwok, Rohit Tripathi, Yu Chen, and Kai Hwang. (August 2005.). HAWK: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks1. -. - (-), p1-10.

[10] Sheetalkumar Doshi Shweta Bhandare Timothy X Brown. (-). An On-demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network. -. 6 (3), p50-66.

[11] Ramesh Govindan and Anoop Reddy . (1995). An analysis Of Internet Inter-Domain Topology and Route stability . -. - (-), p1-22.

[12] Yuto Kawahara Tsuyoshi Takagi and Eiji Okamoto. (-). Ecient Implementation of Tate Pairing on a Mobile Phone using Java. -. - (-), p1-10.

ISSN: 2278 – 7798

[13] Jing Deng, Richard Han, and Shivakant Mishra. (2005,). Defending against Pathbased DoS Attacks in Wireless Sensor Networks. -. - (-), p1-8.

[14] Alexander Kr¨oller S´andor P. Fekete Dennis Pfisterer Stefan Fischer. (2006). Deterministic boundary recognition and topology extraction for large sensor networks. -. 22 (26), p1000-1009.

[15] David B. Johnson , David A. Maltz , Josh Broch. (-). DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. -. - (-), p1-25.

[16] Joppe W. Bos, Dag Arne Osvik, Deian Stefan. (2005). Fast Implementations of AES on Various Platforms. -. - (-), p1-34

[17] Jing Deng, Richard Han, Shivakant Mishra. (2002). INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks. -. 939 (02), p1-18.

[18] Aleksandar Kuzmanovic and Edward W. Knightly. (2003). Low-Rate TCP-Targeted Denial of Service Attacks. -. 25 (29), p75-86.

[19] Xiapu Luo and Rocky K. C. Chang. (-). On a New Class of Pulsing Denial-of-Service Attacks and the Defense. -. - (-), p1-19.

[20] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, Jennifer Rexford. (2008). Path-Quality Monitoring in the Presence of Adversaries. -. 2 (6), p1-12.

[21] Gergely A´ cs, Levente Buttya´n, and Istva´n Vajda. (March 2005). Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks. -. - (-), p1-22.

[22] MINA GUIRGUIS AZER BESTAVROS IBRAHIM MATTA YUTING ZHANG. (-). Reduction of Quality (RoQ) Attacks on Internet End-Systems. -. - (-), p1-11

[23] Yih-Chun Hu David B. Johnson Adrian Perrig. (-). SEAD: Secure Efficient Distance Vector Routing for MobileWireless Ad Hoc Networks. -. - (-), p1-11.

[24] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. (-). Strong Authentication for RFID Systems Using the AES Algorithm. -. - (-), p1-14.

[25] John R. Douceur. (-). The Sybil Attack. -. - (-), p1-6.

[26] Leonardo B. Oliveira, Diego F. Aranha, Eduardo Morais, Felipe Daguano,Julio L´opez,Ricardo Dahab. (-). TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes. -. - (-), p1-6.

[27] Rodrigo Fonseca Sylvia Ratnasamyy Jerry Zhaoz Cheng Tien Ee David Culler Scott Shenker;z Ion Stoica. (-). Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets. -. - (-), p1-14.

First Author: E. GAYATHRI, Research Scholar, Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapuramu, Andhra Pradesh, India.

Second Author: Dr. N. Geethanjali, Associate Professor, Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapuramu, Andhra Pradesh, India.

ISSN: 2278 – 7798