ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

An Intrusion Detection System in MANET

B. Abinaya[1]

M.E. Software Engineering, University College of Engineering, Tiruchirapalli, Bit Campus, Mandaiyur, Trichy, India

ABSTRACT: Wireless Sensor Network (WSN), a fast growing network scheme and it provides lots of features to communication strategies and routing protocols. Energy efficiency and Security Maintenance is a challenging task to resolve in Wireless Sensor Networks because of dynamic route establishment and route maintenance schemes especially in MANET the complexity is comparatively high. In this system, an AODV based LDK model is implemented to define the intrusion free routing environment with set of nodes and provide the energy efficient routing scheme as well as implementing the data security parameters with the help of Advanced Cryptographic Standard (AES) algorithm. This AES algorithm is operated under 256-bit encryption mechanism and providing powerful data security scheme over transmission data. So that the source and destination can perform trustworthy data transmission in energy efficient manner. The entire transmission is held over by Intrusion Detection and Prevention Systems and before starting transmission we perform the strength manipulation for every node presented into the network and select the path dynamically using Game Theoritic Modeling, which calculates the energy for all nodes to transmit corresponding data over wireless sensor network. In this system LDK methodology is used to identify the best route that means once the source node starts transmission it estimates the nearest node and start transmitting data via the respective Neighbor Node (NN). If any node interrupting the active nodes while communication, which will be considered as a malicious node and the routing environment eliminate that particular node from transmission further by marking it as a malicious/intruder node in Routing Table. For all the entire system is used to perform the efficient intrusion free communication between source and destination via two powerful methodologies such as Game Theoretic Modeling with LDK and Advanced Encryption Standard mechanisms.

KEYWORDS: Ad Hoc Networks, MANET, Intrusion Detection, Energy Efficiency.

I. INTRODUCTION

MANET is a self-sorted out accumulation of portable hubs which speak with each other without the assistance of any settled foundation or focal facilitator. A hub can be any cell phone with the capacity to speak with different gadgets. In a MANET, a hub carries on as a host and a switch. A hub planning to speak with another hub that is not inside its correspondence extend, takes help of halfway hubs to hand-off its message. The topology of the system powerfully changes after some time as hubs move about, some new hubs join the system or couple of different hubs separate themselves from the system. MANETs have unmistakable points of interest over conventional systems in that they can without much of a stretch be set up and disassembled, aside from giving adaptability as the hubs are not fastened. Other than being operable as a remain solitary system, impromptu systems can likewise be joined to the Internet or different systems, in this manner expanding network and scope all the more imperatively to ranges where there are no settled foundations. Present and future MANET applications cover an assortment of ranges. One essential application situation is VANET.

VANET is a self-arranging system of moving vehicles (i.e., a vehicle is a hub) in spite of the fact that the development example of hubs are limited by the street course, movement controls, and so on. VANET is a promising innovation that can possibly enhance vehicle and street wellbeing, movement proficiency and comfort. Because of the inborn attributes of a MANET, for example, versatility, remote correspondence connections and absence of any brought together expert, giving security in a MANET is a testing assignment. In addition, security answers for settled wired systems are not effortlessly versatile to portable remote systems. One method for giving security to a MANET is interruption discovery, a procedure of checking exercises in the framework in order to figure out if there has been any

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

infringement of security necessities. Intrusion Detection System (IDS) is the instrument utilized by the hubs of a system for recognition of interruption and has been characterized into two general classifications in view of the strategies embraced, viz., (a) Signature-based interruption location and (b) Anomaly-based interruption discovery.

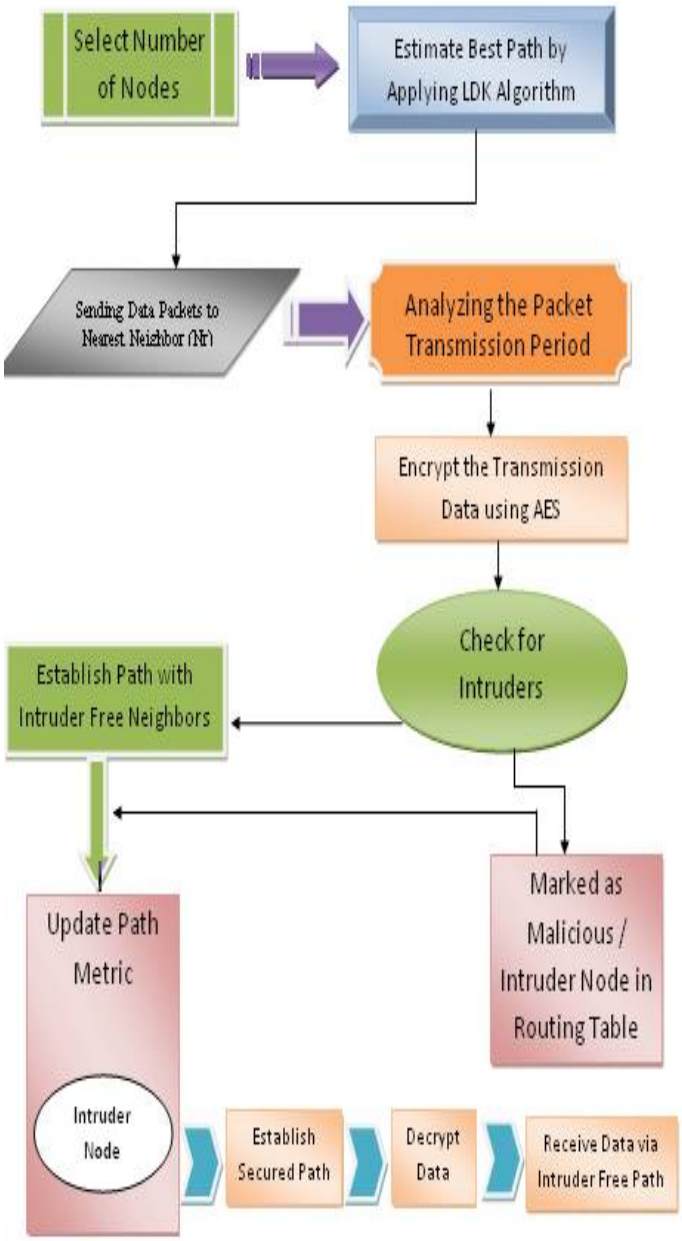

Fig.1 System Architecture Design

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

II. EXISTING SYSTEM

In MANET, inherent characteristics such as mobility, wireless communication links and lack of any centralized authority, providing security in a MANET is a challenging task. Moreover, security solutions for fixed wired networks are not easily adaptable to mobile wireless networks. One of the most affecting security threats in MANET is intrusion system. At the occurrence of an attack, the characteristics of the attack are matched with the signatures included in the IDS. If there is a match, then an attack associated to that signature is said to have occurred. So a new mechanism is required to resolve these issues.

MANET plays a vital role in Wireless network area, which is threatened by a lot of security attacks such as denial of service attack, modification, IP spoofing, fabrication attack, etc. The Intruder based attack has a serious impact on reactive routing protocols. In intrusion attacks, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages.

In this case, an intruder node (so-called malicious node) can attract all packets by using forged route synchronization packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination.

Disadvantages:

- Providing Security to MANET is a challenging task.
- Malicious information broadcasting is a crucial task in MANET.
- Security is less.
- Performance is low.

III. PROPOSED METHODOLOGY

The proposed approach focuses on attack free MANET based wireless communication medium with the help of DSR Protocol. The proposed protocol determines two main functionalities: (a) Security and (b) Trustworthy Communication. In proposed system Intrusion Detection System (IDS) is introduced, which is the mechanism used by the nodes of a network for detection of intrusion and has been classified into two broad categories based on the techniques adopted, viz., (a) Signature-based intrusion detection and (b) Anomaly-based intrusion detection. In signature-based detection, knowledge about the signatures of attacks is incorporated in the detection system. In proposed approach Source Node identifies the nearby node called neighbors dynamically by using Game Theoretic approach. The nearby node checks it and forward route reply to Source/parent Node. If so the neighbor node is a proper node. In neighbor node sequence Number will incremented by 1 count. If the node is proper then only the count will be incremented otherwise it consist intrusion. Selecting Neighbors based on Shortest Path, so the performance is good as well. If any intruder tries to communicate with the active nodes that nodes are marked as intruder nodes in Routing Table.

Advantages:

- Security is highly concentrated via improvised LDK algorithm and Game Theoretic Modeling.
- Information broadcasting is more secured compared to the existing system.
- Security is high and Performance is improved.

Algorithm 1: LDK

Step 1.Each node M broadcasts a message of type Send-Degree to its neighbors asking them to send their degree. M− > broadcast : (SendDegree)

Step 2.On receipt of the SendDegree message in step 1, each neighbor node, B of M replies to M a ReplyDegree message. B− > M : (ReplyDegree)

Step 3.On receipt of each ReplyDegree message in step 2, M does the following:

i. For each message do degree = ReplyDegree;

ii. k = Minimum(degree);\

iii. If l > k then pmin M = 1. Otherwise, pmin M is assigned the minimum value of p (where l is the desired security level of the neighbor, T +ϱ=1, ϱ is a very small positive number) such that k Xi=l ↕ k i‼ pi(1 − p)k−i ⊥ T

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

IV. LITERATURE SURVEY

In the year of 2012 the authors "S. Zeadally, R. Hunt, Y-S. Chen, A. Irwin and A. Hassan" described into their paper titled "Vehicular ad hoc networks (VANETS): status, results, and challenges" such as recent advances in hardware, software, and communication technologies are enabling the design and implementation of a whole range of different types of networks that are being deployed in various environments. One such network that has received a lot of interest in the last couple of years is the Vehicular Ad-Hoc Network (VANET). VANET has become an active area of research, standardization, and development because it has tremendous potential to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers.

Recent research efforts have placed a strong emphasis on novel VANET design architectures and implementations. A lot of VANET research work have focused on specific areas including routing, broadcasting, Quality of Service (QoS), and security. We survey some of the recent research results in these areas. We present a review of wireless access standards for VANETs, and describe some of the recent VANET trials and deployments in the US, Japan, and the European Union. In addition, we also briefly present some of the simulators currently available to VANET researchers for VANET simulations and we assess their benefits and limitations. Finally, we outline some of the VANET research challenges that still need to be addressed to enable the ubiquitous deployment and widespead adoption of scalable, reliable, robust, and secure VANET architectures, protocols, technologies, and services.

In the year of 2010 the authors "S. Marti, T. J. Giuli, K. La and M. Baker" described a paper titled "Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment" such as this system describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection.

When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead.

In the year of 2003 the authors "K. Nadkarni and A. Mishra" described into their paper titled "Intrusion Detection in MANETs - The Second Wall of Defense" such as Wireless mobile ad hoc networks (popularly known as MANETs) have been the focus of research in recent times. Rapid and infrastructure-less deployment in emergency and military situations make these networks unique.

However, certain inherently vulnerable characteristics lead to security concerns, which can prove especially damaging in sensitive situations like military operations. Intrusion prevention measures are not guaranteed to work all the time since unrelenting attackers can eventually break them down. An intrusion detection scheme (IDS) monitors a network and looks for intrusions, thus forming a second wall of defense. In this paper, we have proposed a misuse detection -based IDS for MANETs. Our protocol-independent design makes use of a self-adjusting threshold scheme and detects a priori known attack patterns with over 90% accuracy and is generally insensitive to false alarms. Experimental validation has provided significant results about non-degradability of network performance with our IDS incorporated for security enhancements.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

V. EXPERIMENTAL RESULTS

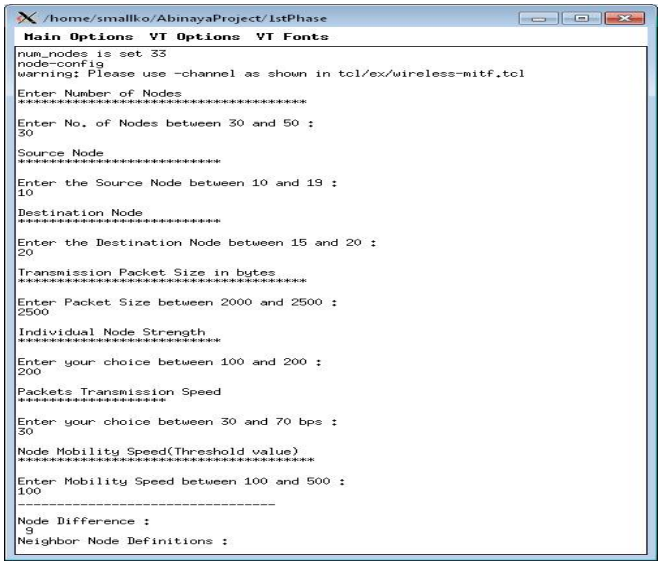

Fig.2 Input Parameters

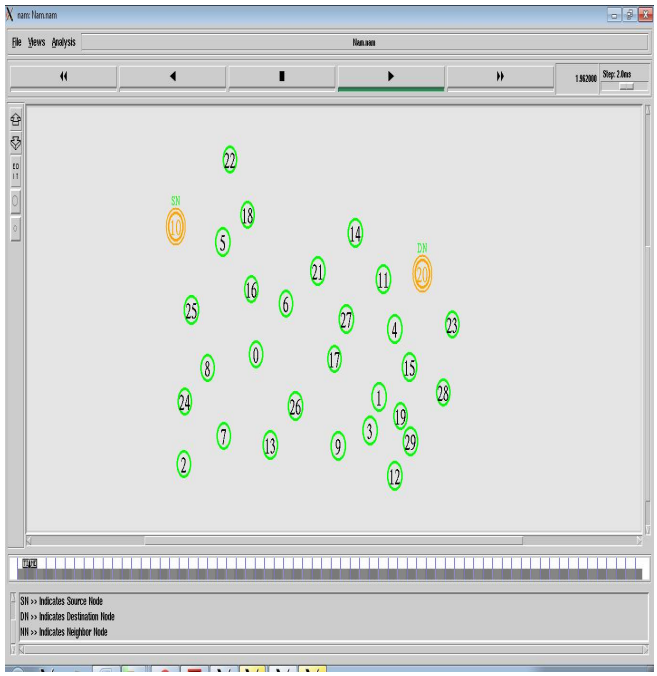

Fig.3. Wireless Node Formation

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

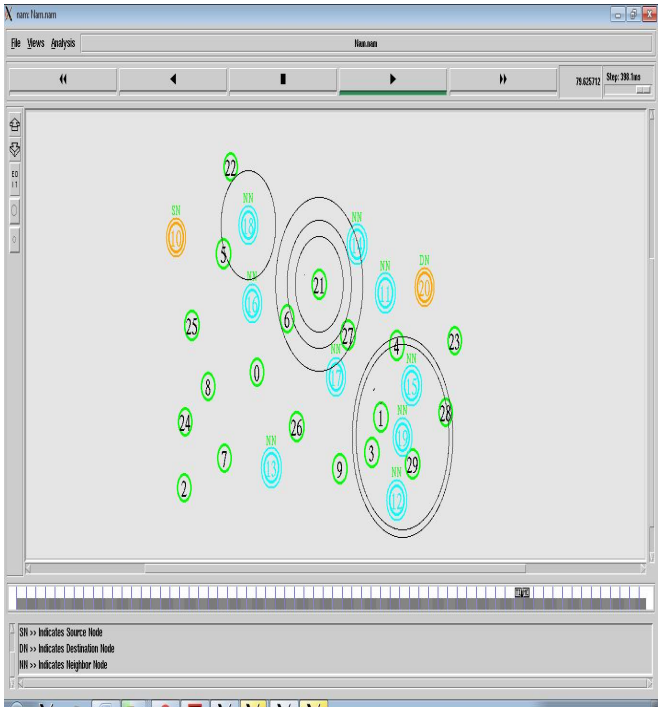

Fig.4. Finding Intruders

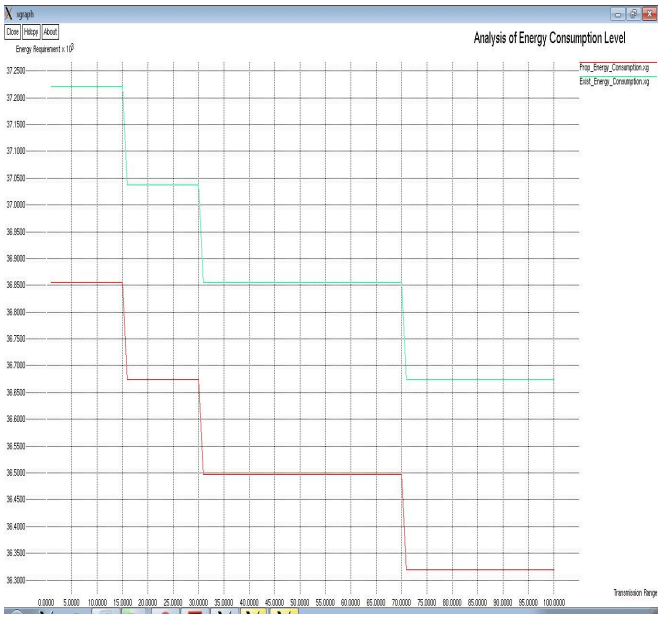

Fig.5. Energy Consumption Model.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VI. CONCLUSION AND FUTURE SCOPE

In this approach we have proposed an efficient way of using intrusion detection systems (IDSs) that sits on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. We then described a cooperative game model to represent the interactions between the IDSs in a neighborhood of nodes. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighborhood at a desired security level so as to detect any anomalous behavior, whereas, the secondary goal of the IDSs is to conserve as much energy as possible. To achieve these goals, each of the nodes has to participate cooperatively in monitoring its neighbor nodes with a minimum probability. We then develop a distributed scheme to determine the ideal probability with which each node has to remain active (or switched on) so that all the nodes of the network are monitored with a desired security level.

The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (a) keeping IDSs running throughout the simulation time and (b) using our proposed scheme to reduce the IDS's active time at each node in the network. From the simulation results we observe that the effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. Here we have assumed a homogeneous network in a way that all the nodes have the same capacities in terms of their computational and energy resources. In future we wish to extend our model to accommodate a heterogeneous network.

REFERENCES

[1] S. Zeadally , R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.
[2] S. K. Bhoi and P. M. Khilar, "Vehicular communication: a survey", IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.
[3] S. Marti, T. J. Giuli, K. La and M. Baker, "Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment," Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, August 2000.
[4] C. Manikopoulos and L. Ling, "Architecture of the Mobile Ad-hoc Network Security (MANS) System," Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3122- 3127, October 2003.
[5] K. Nadkarni and A. Mishra, "Intrusion Detection in MANETs - The Second Wall of Defense," Proc. IEEE Industrial Electronics Society Conference '2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.
[6] A. Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad-hoc Networks," Proc. 3rd IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March 8-12, 2005.
[7] N. Marchang and R. Datta, "Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks," IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.
[8] N. Marchang and R. Datta, "Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks," Elsevier Ad Hoc Networks, vol. 6, no. 4, pp. 508-523, June 2008.
[9] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, "Edge Self-Monitoring for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems," vol. 22, no. 3, March 2011, pp. 514-527.
[10] I. Khalil, S. Bagchi and N. B. Shroff, "SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks," Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007 (DSN 2007), 565-574.
[11] T. Hoang Hai and E-N. Huh, "Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks," Proc. Future Generation Communication and Networking (FGCN 2007), vol.1, no., pp.350-355, 6-8 Dec. 2007.
[12] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu, "On modeling energysecurity trade-offs for distributed monitoring in wireless ad hoc networks," Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1-7, 16-19 Nov. 2008.
[13] R. G. Clegg, S. Clayman, G. Pavlou, L. Mamatas and A. Galis, "On the Selection of Management/Monitoring Nodes in Highly Dynamic Networks," IEEE Transactions on Computers, vol.62, no.6, pp.1207-1220, June 2013.
[14] R. Zheng, T. Le and Z. Han, "Approximate Online Learning Algorithms for Optimal Monitoring in Multi-Channel Wireless Networks," IEEE Transactions on Wireless Communications, vol.13, no.2, pp.1023-1033, February 2014.
[15] N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, "LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System," IEEE Transactions on Emerging Topics in Computing, Vol. PP, no. 99, 2014.

BIOGRAPHY

Ms. Abinaya. B. Studying M.E. Software Engineering in University College Of Engineering Or Anna University Tiruchirapalli,Bit Campus, Mandaiyur, Trichy, 620024.