ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Utilization of Energy from Attacks Using RSA Algorithm in Wireless Ad hoc Sensor Network

[1]Rashmi, [2]Dr. R Kanagavalli

M.Tech II Year Student (CNE), Dept of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

Professor, Dept of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Wireless sensor network consists of small sensing devices which collaborate with each other to gather process and communicate over wireless channel information about some physical phenomena. These are self-organizing, highly robust and energy efficient network that can be excellent sentinels for monitoring underground mining, wildlife and various physical infrastructures such as buildings, pipelines and bridges. This paper explores the resource depletion attacks which will permanently disable network by draining nodes battery power. The concept PLGPa protocol was used to overcome the security issues in the existing. Using PLGPa, the data which is transferred will be hacked by the attacker. Hence, we are proposing RSA algorithm which is asymmetric in nature as well as alternate path. The proposed algorithm will consume less energy and the path established from source to destination will be secured.

KEYWORDS: Deniel Of Service, Sensor Networks, Wireless networks, Ad Hoc Networks, Routing Protocols, Security requirements, Network layer attacks**.**

I. INTRODUCTION

Wireless Ad-hoc network is a decentralized network which is a collection of wireless mobile [4] nodes that self-configure to form a network without the aid of any established infrastructure. The nodes are equipped with wireless transceiver. Therefore, each node doesn't only plays the role of an end system, but also acts as a router, that sends packets to desired nodes. Ad-hoc networks [2] are vulnerable to DOS attacks which lead to the resource depletion. MANET routing protocols are designed to focus on the efficiency and performance of the network [1]. Ad hoc [5] network are wireless network with no fixed infrastructure in which nodes depend on each other to keep the networked connected. Topology based routing protocols use the information about links for packet forwarding. Position based routing protocols use node's geographical position to make routing decisions. Dynamic Source Routing (DSR) protocol is the most widely used protocol. As the sensor networks are generally used in sensing sensitive information their efficiency is of major concern. Their performance depends upon three tasks of sensing, data gathering and routing of the information to the sink. Vampire attacks are the form of attacks on consumption of life from the network through they do not disrupt immediately availability, they work overtime to disable the network entirely.

II. LITERATURE SURVEY

Detection mechanisms that have been proposed so far can be grouped into two broad categories.

1) Proactive detection schemes are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage.
2) Reactive detection schemes are those that trigger only when the destination node detects a significant drop in the packet delivery ratio. Many existing protocols are used namely DSR, AODV, OLSR.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

DSR protocol [1] is a reactive protocol which means it is a on-demand protocol. It is based on the concept of source routing i.e., the source will specifies the entire route to be taken by the packet during transmission from source to destination instead of the next hop. If the source node does not have the route then it floods the network with a Route Request (RREQ). Any node which has a path to the destination can reply with the Route Reply (RREP) to the source. This reply contains the entire path which is recorded in the source. The existing secure sensor network routing protocol by Parno et al. was used for the security purpose. But this protocol was consuming more energy due to attacks such as stretch attack and carousel attack. It also leads to low security level. To overcome this we are proposing RSA algorithm with alternate path. RSA algorithm is a security algorithm and it consumes less energy in the network during transmission of packets from source to destination. In the existing we used PLGP with attestations. It leads to less security.

III. PROPOSED WORK

In the proposed, we are using the security [9] algorithm called RSA which is asymmetric in nature. Symmetric means it consists of two keys i.e., Public key and Private Key. The public key is known to all but the Private Key will be known only to the destination. The RSA [10] consists of three steps such as Key generation, Encryption and Decryption. At the source the key is generated and this information will be encrypted after the generation. This encrypted information is then passed on to the other nodes. When the attacker attacks the node, he will not be able to decrypt the information sent. Finally, the information or encrypted information will reach the destination and the destination will decrypt that with the help of private key. If ever there is an attacker attacking the node then that node will be discarded using distance formula so that it will choose an alternate path. We are enhancing this approach in NS-2[3].

Preventing Vampire Attacks Using PLGPa: Vampire Attacks problem can be overcome using PLGPa protocol. In the existing, PLGP protocol is used. The proposed algorithm called RSA will provide security and transfer the packets to the destination. The proposed algorithm will ensure the security by using the encryption from source to sink

IV. SIMULATION RESULTS

The simulation studies involve the network topology where we consist of 38 nodes in the network which is mobile in nature as shown in the Figure 1. We are performing simulation using NS-2. After the nodes are deployed in the network they start broadcasting the presence with the neighbouring nodes as shown in Figure 2. When all nodes finish broadcasting the source node start sending the RREQ and finally when sink node receives it, it will reply back by sending RREP by establishing the shortest path as shown in Figure 3. The source node starts sending the encrypted data through the shortest path. The attackers come in to the picture and start attacking the nodes as shown in the Figure 4. The source node will wait for acknowledgement and when it does not receive it understands that some nodes have been attacked and will send data using alternate path or route. Hence we calculate energy consumption as shown in the Figure 5 and end-end delay as shown in the Figure 6 using this simulation and finally obtain graphs. We calculate how much energy is consumed and compare it with the existing as well as the proposed one then the graph is obtained.

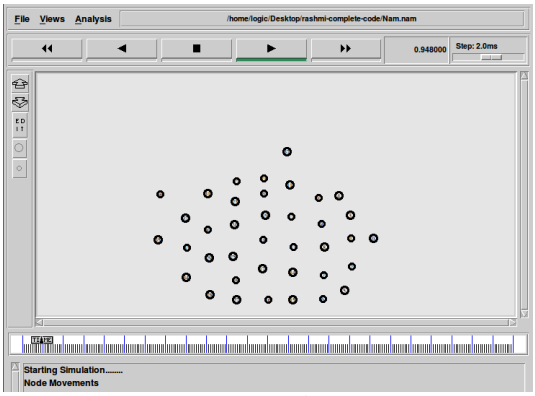

Figure 1: Deployment of nodes

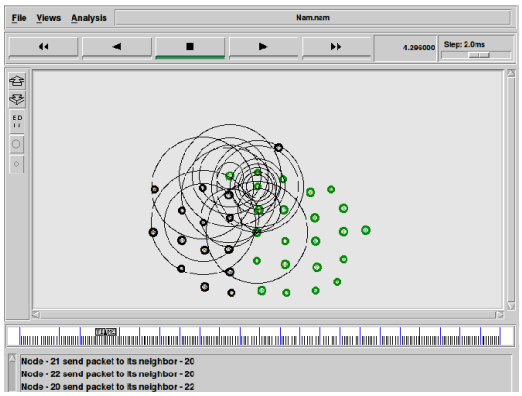

Figure 2: Broadcasting the message

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

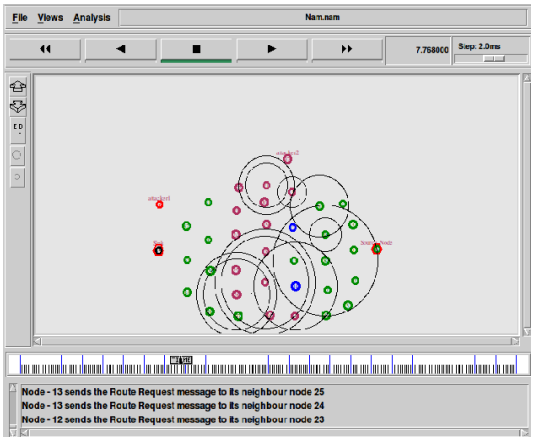

Figure 3: RREP message and RREP messages

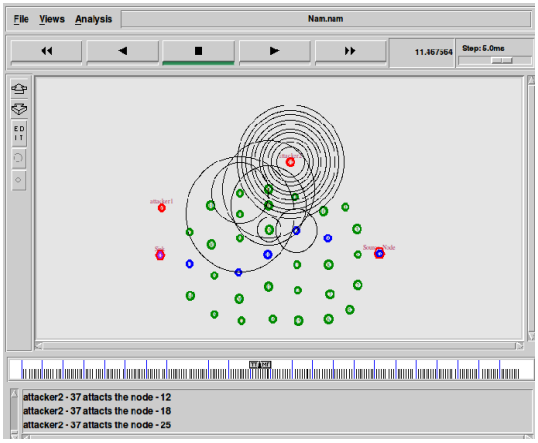

Figure 4: Attacker attacking the nodes

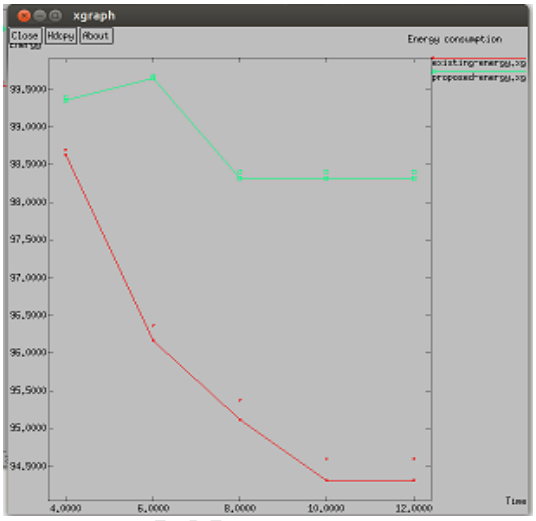

Fig.5: Energy consumption

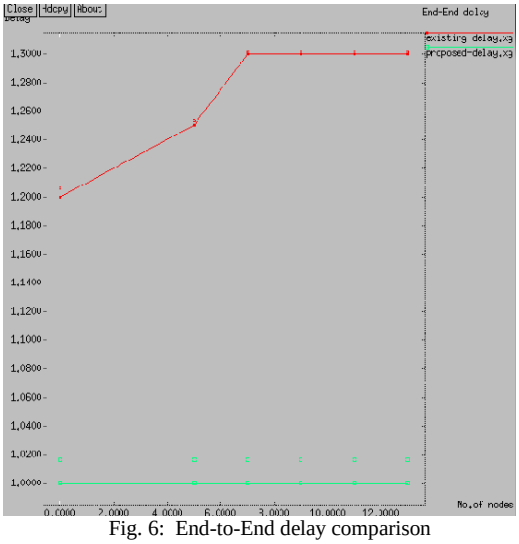

Fig. 6: End-to-End delay comparison

V. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network. Security is the most important feature for deployment in Ad hoc network. The misbehavior of the nodes will cause severe damage to the whole network. In order to overcome the security issues we are using the RSA algorithm as well as alternate path. The main goal of using these is to improve the security as well as the performance of the network.

REFERENCES

1. P Narayan, V R. Syrotiuk ,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool," *in the proceeding or ADHOC-NOW* in the year o 2004.
2. M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocol" i*n the proceeding of 3rd ACM workshop on Wireless Security in the year of* 2002.
3. Harish Kumar, Harneet Arora, "Simulation Analysis Of Optimized Link State Routing Protocol in Wireless Sensor Networks," *in the year 2011.*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

4. Amit Jardosh, Elizabeth M. Belding-Royer, Kevin C.lmeroth and Subhash Suri, "Towards Realistic Mobility Models for Mobile Ad- hoc Networks", MobiCom'03, September 14-19, 2003.
5. C. Kim, E. Talipov, and B. Ahn, "A reverse aodv Routing protocol in ad hoc mobile networks," in Proceedings of the 2006 international conference On Emerging Directions in Embedded and Ubiquitous Computing, ser. EUC'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 522–531. [Online].Available http://dx.doi.org/10.1007/11807964-53.
6. A. Hamidian, U. K¨orner, and A. Nilsson, "Performance Of internet access solutions in mobile ad hoc networks," In Proceedings of the First international conference on Wireless Systems and Mobility in Next Generation Internet, ser. NGI'04. Berlin, Heidelberg: Springer- Verlag, 2005, pp. 189– 201. [Online]. Available: http://dx.doi.org/10.1007/ 978-3-540- 31963-4-14
7. Z. M. M. Said Khelifa, "An energy reverse aodv Routing protocol in ad hoc mobile networks, in World Academy of Science, Engineering and Technology 68 2010, 2010.
8. ELMurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkhyu Ha, YoungJun Choi, and Chonggun Kim, Path Hopping Based on Reverse AODV for Security, Sringer, APNOMS(2006).
9. Ali Modirkhazeni, Norafida Ithnin, Othman Ibrahim, "Secure Multipath Routing Protocols in Wireless Sensor Network: A Security Survey Analysis." *2010 IEEE.*
10. Seys, E. "*Lightweight Cryptography Enabling Secure Wireless Sensor Network , Security Issues In Mobile And Wireless Heterogenouse Networks.*2004.
11. Li, P., Zhang , J., & Lin, Y.-P. Curve-Base Routing Algorithm for Sensor Networks. *International Conference On Computer Networks And Mobile Computing.* 2005.

BIOGRAPHY

Rashmi is a student of Information Science and Engineering Department at The Oxford College of Engineering-Bangalore, affiliated to VTU pursuing M.Tech in Computer Networking and Engineering. She received her Bachelor's of Engineering in Computer science and Engineering from S L N College of Engineering-Raichur affiliated to VTU. She is currently pursuing M.Tech (CNE), The Oxford College of Engineering, Bangalore under the guidance of **Dr. R. Kanagavalli.**

Dr. R. Kanagavalli got UG in Bharathiar University, Coimbatore, Tamil Nadu. She got PG and PhD in Anna University, Chennai. She has an experience of 12 years in teaching field. She had completed B.E, M.E and PhD in Computer Science and Engineering. Currently she is Professor for Information Science and Engineering department at The Oxford College of Engineering, Bangalore, affiliated to VTU. Her research interests are Image processing and video processing. She has published around 12 papers including both International Conference and International Journal.