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. 4, April 2014, pg.836 – 840

RESEARCH ARTICLE

A NOVEL METHOD FOR SECURE ROUTING WITH EFFICIENT ENERGY RESOURCES IN WIRELESS NETWORK

[1]Ms. G.Subbulakshmi @ Nithya, [2]Mrs. J.Priskilla Angel Rani

[1]PG Student, [2]Assistant Professor

[1&2]Francis Xavier Engineering College, Tirunelveli-627003, Tamilnadu, India

[1] subbulakshminithya@gmail.com, [2] pricy.angel@gmail.com

Abstract- An ad-hoc wireless network is significant among other wireless networks. A base station links the sensor network to another network to disseminate the packets sensed for further processing. The assigned packets are sent from source to sink. By this time the adversary can attack the packets and deplete the node's energy. So the original content will differ. Thus, the node's battery power is diminished. To overcome this disadvantage, the honest node is detected using DSDV protocol. By this, the lifetime of the ad-hoc nodes is extended. Also RSA algorithm is used here for security purpose.

Index terms: DSDV protocol, carousel attack, stretch attack

I. INTRODUCTION

A wireless Ad-hoc sensor network is a distributed self-directed network using sensors to observe the physical conditions. Wireless ad-hoc sensor network is a collection of nodes, each of which has the characteristic such as transmit and receive messages over communication links, wireless or cabled. In ad-hoc society, wireless ad-hoc networks are helpless to denial of service attacks [2]. The denial of service attack is to entirely reduce node's energy. This is an example of a resource depletion attack [1]. Ad-hoc nodes have less node failure when compared to sensor node. Thus node topology does not change frequently. These networks found application in areas such as medical monitoring, land slide detection and in some military applications.

The important resource of wireless Ad-hoc sensor network is the energy, which is used to find out the network's life time. In order to increase the life time of the network, the energy consumption must be reduced since each node in the network will be energy efficient. To make the node energy efficient, shortest path routing with less number of intermediary nodes is considered for transmission purpose.

II. EXISTING SYSTEM

In existing system there are two main problems are available. They are stretch attack and carousel attack. Carousel attack means sources node transmit the messages to sink node with destination address by using the DSDV (Destination Sequence Distance Vector). But here some loops are occurred so the message repeatedly

moves on the loop it does not receive to sink at correct time. So the large amount of energy will be reduced randomly. Second one is stretch attack here the distance path will be chosen. Thus large amount of energy is reduced. To overcome this problem, the honest node method is used. This is the mitigation method of these energy consumption problems. In this method it will choose the exact path (shortest path). So the energy usage is perfect and correct. But here there is no security available.

III. PROPOSED SYSTEM

Here two main attacks are available they are Stretch attack and Carousel attack. In these attacks energy will be reduced to recover using honest node method to improve the energy but security level is low so using RSA algorithm to improve the security level. This algorithm was proposed by Ron Rivest Adi Shamir Adleman. This algorithm is an asymmetric algorithm having two way protections. Here both private and public keys are generated. Key size is according to the file size. Public key is visible to all but private key is visible to only receiver. First Split the file into number of pieces. This fragmented files encrypted with public key but it does not open with public key it open only with private key. Decrypt the file using private key securely.

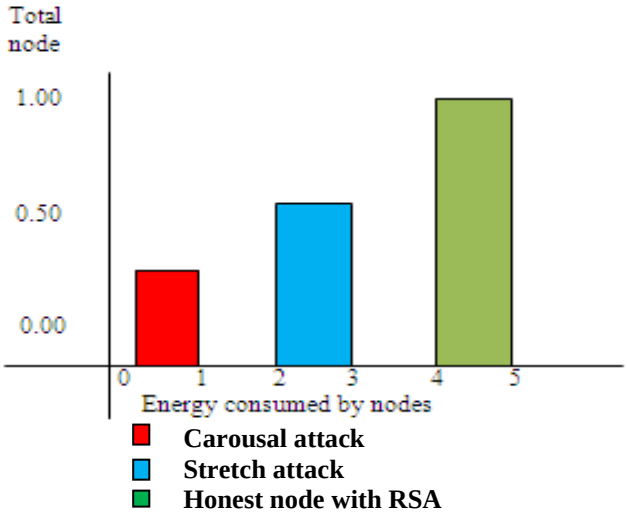

Fig: 1 Graph with RSA Algorithm

IV. SYSTEM ARCHITECTURE

Source node sent many messages to sink node. At that time adversary attacks the message content and it creates loop (i.e.) change the path. After this, the message transmitted by the source node will be received by the sink node. Even then there are different types of problems will occur such as poor security. So to avoid this, RSA algorithm is used to encrypt the message and is transmitted through communication channel which cannot be read from outside adversaries. Source node will use the public key for encryption (Fig: 3) and the sink node will use the private key for decryption (Fig: 4).

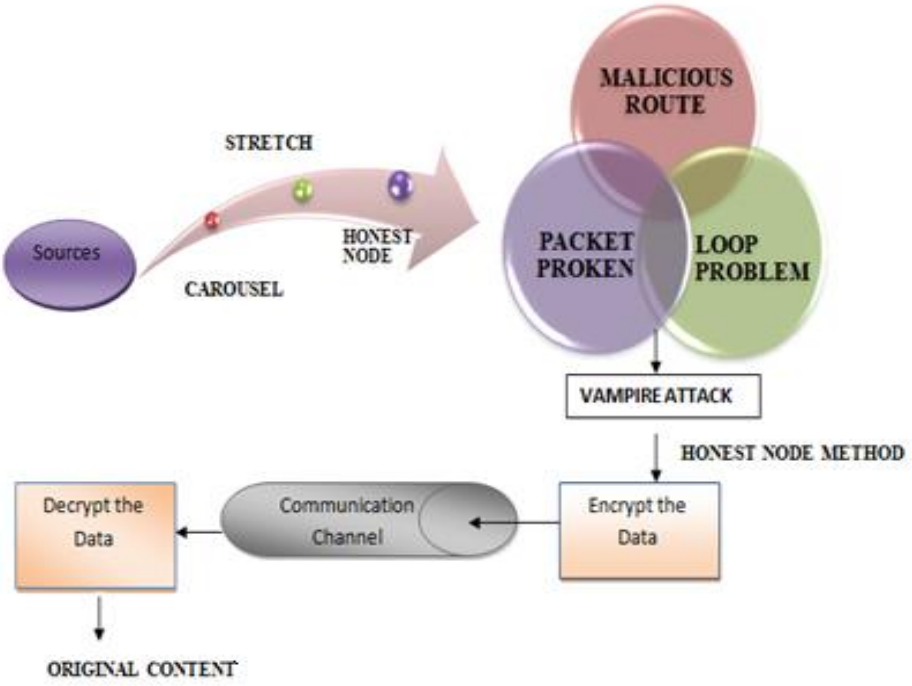

Fig: 2 System Diagram

V. RESULTS

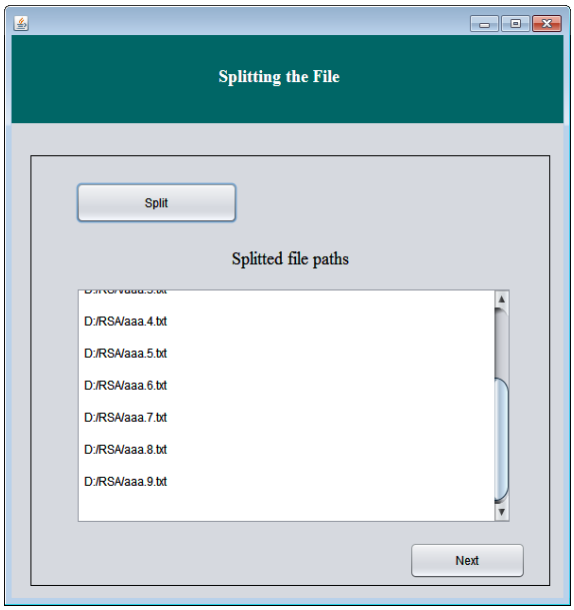

Fig: 3 Splitting File

The file is splitted into small pieces and different paths are assigned to reach the sink node. These splitted files are encrypted and couldn't be read by unauthorized person.

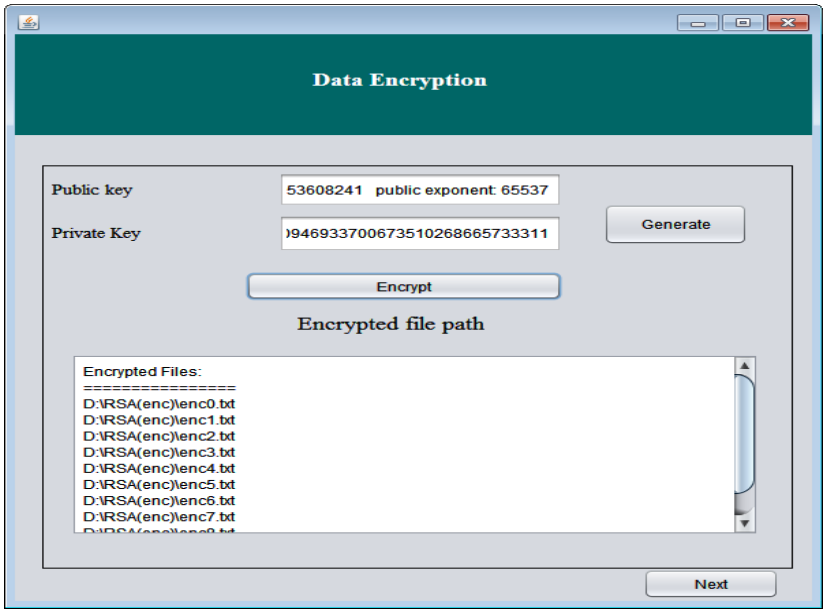

Fig: 4 Data Encryption

Keys are generated both public and private for encryption and decryption. After that, encrypt the files with assigned path. Encrypted files stored in D drive.

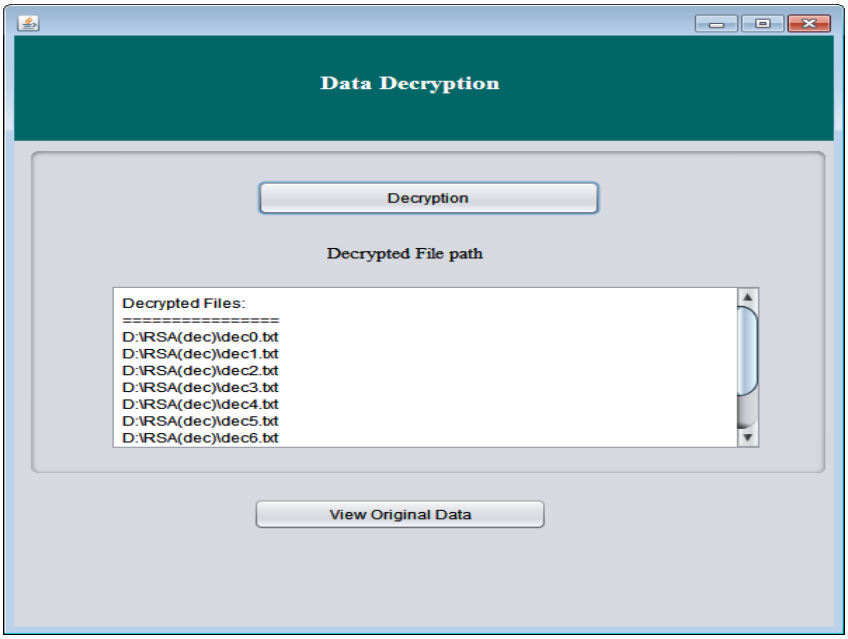

Fig: 5 Data Decryption

Here is the sink node to decrypt the message with private key. The sink node is the only node that will have the private key for decryption and thus this algorithm provides high security.

VI. CONCLUSION

The conclusion is that the energy consumption of node is highly reduced using the proposed algorithm. Simulation result shows that depending on the location of the adversary, network energy expenditure increases from 50 to 1,000 percent during the forwarding phase. Then the RSA algorithm has been used for encryption and decryption of the splitted message and the problem in the existing system is solved.

ACKNOWLEDGMENT

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. We express our gratitude to all our well wisher who really motivates us in publishing this paper.

REFERENCES

[1]. Eugene Y. Vasserman and Nicholas Hopper " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", VOL. 12, NO. 2, FEBRUARY 2013
[2]. A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.
[3]. Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad-hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.
[4]. Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.
[5]. John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.
[6]. Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.
[7]. Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.
[8]. I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.
[9]. Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.
[10]. Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.
[11]. T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and Marnane, "A Low-Power Pairing-Based Cryptographic Accelerator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.
[12]. L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.
[13]. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm, "Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES), 2004.
[14]. T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.
[15]. T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and W. Marnane, "A Low-Power Pairing-Based Cryptographic Accelerator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.
[16]. www.google.com

AUTHOR(S) PROFILE

G. Subbulakshmi @ Nithya is doing M.E Network Engineering in Francis Xavier Engineering College, Tirunelveli. She completed her B.E., Computer Science and Engineering in Francis Xavier Engineering College, Tirunelveli in the year 2012.She is a member in Computer Society of India. Her areas of interest are Cryptography, Wireless Networks and Mobile Computing.

Mrs. J. Priskilla Angel Rani had completed her B.E., Computer Science and Engineering in Jayaraj Annapackiam C.S.I College of Engineering, Nazareth in the year of 2005. She had completed her M.E., Computer Science and Engineering in Arulmigu Kalasalingam College of Engineering, Krishnankoil in the year of 2008. Her areas of interest are Mobile Computing and Networking.

