International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | April-2016 www.irjet.net p-ISSN: 2395-0072

Latency Reduction with Cryptography based security in MANETs

Neha Ingley[1], Prachi Gawande[2]

[1]Assistant Professor, Dept. Electronics Engineering, YCCE, Maharashtra, India
[2]Assistant Professor, Dept. Electronics & Telecommunication Engineering, YCCE, Maharashtra, India

---

Abstract - *Industrial application of wireless sensor networks require timelines in exchanging messages among nodes. To achieve low latency, high performance wireless links are used which resolves the mechanical problem of wired links. AODV was designed specifically for wireless mobile nodes communicating in an ad-*hoc *fashion to find routes on an as needed basis with minimal route acquisition latency and control overhead. In addition to that networks are being used in various areas, MANET is one of them, as the nodes communicate with each other by sending the data using AODV routing protocol. Network gets affected by various types of attacks. For removal of attack RC-6 algorithm have been used. The drawbacks of DSDV routing protocol are overcome by reactive routing protocol named AODV. The failure of the link will degrade its characteristics as when the error message is sent back to source and the process get repeated. In this chapter, we are proposing a method when nodes or links fails to receive the data packets. Cryptography technique RC6 is used to secure the network.*

***Key Words*: Cryptography, Mobile ad-hoc network, NS2, Routing protocol, RC6, Security, AODV, Delay, Jitter, NS2, Throughput, Latency**

1. INTRODUCTION

In Ad-hoc networks, two or more wireless mobile nodes agree to pass packets for each other. Ad hoc on demand distance vector (AODV) is one of the frequently used routing protocol and network is established. Normally in any network, communication occurs due to presence of central node. But in case of MANET, communication takes place even in absence of central node. AODV is used to analyze the different attacks on network and to reduce the latency of wireless sensor network. In this chapter, we are going to check performance parameters, evaluation parameters and analysis of attack.

1.1 LATENCY

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. For analysis of latency, delay, Throughput , jitter, PDR, energy are the factors that need to be considered.

1.1.1 Delay

Network delay is very important parameter in telecommunication network. Delay specifies how much time node requires sending data.

1.1.2 Throughput

Throughput is the rate at which message is delivered successfully.

1.1.3 PDR (Packet Delivery Ratio)

PDR is the ratio of number of packets received and number of packets sent. The greater value of packet delivery ratio implies the better performance of the protocol.

1.1.4 Jitter

Jitter is generally observed in the form of characteristics of successive pulses.

1.2 Types of Attacks

Internal attacks: The attacker acts one of the nodes from the containing nodes and gains direct access to the network and can do the malicious activity.
External attacks: The attacker attacks from outside the network in this type, due to congestion in the network traffic by propagating non meaningful messages throughout the network, thereby disturb the entire communication of the network.

1.2.1 Impersonation

This type of attack is fall in the category of the most severe attacks. The attacker can act as an innocent node and join the network in this type of attack. Similar way, when several this type of nodes join the network, they gain the full control of the network and conduct malicious behavior. They spread fake routing information and they also gain access to confidential information. A network is vulnerable to such attacks if it does not employ a proper authentication mechanism.

1.2.2 Denial of Service

This type of attack is first making sure that a specific node is not available for service. So the entire service of the network might be disturbed due to this attack.

1.2.3 Eavesdropping

The main goal of the attacker is to get some private information in this type of attack, while it is being transferred from one node to the other. This attack is very much complex to find out and the secret information like private and public key password etc. of the nodes can get compromised due to this attack.

1.2.4 Black hole attack

A black hole is created with the opponent at the main Centre. The opponent traps the traffic of the network close to a compromised in this type of attack. Basically the attacker offers an attractive path to the neighboring nodes. This attack can also be paired with other attacks like packets dropping, denial of service, replay of knowledge, selective forwarding.

1.2.5 Wormhole attack

Here the opponent connects two distant parts of the network and convey messages received in different part of the network to the other. A lower latency link is used to pass the messages in this type of network.

1.2.6 Sybil attack

In this type of an attack, a particular node in the network tries to have several different fake identities. Thus this way helps the malicious node to gain more and more specific information about the network. The validness of fault tolerant schemes like; multipath topology in routing, distributed storage, maintenance has a great decrease.

1.3 Routing Algorithm- AODV

The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. Previously like in dynamic source routing , the packets were sent to all nodes in the network regardless of whether it is required or not. Hence packet of data has to follow all routes resulting delay. Along with delay the throughput and energy are affected which cause to overlap or congestion problem in a wireless mesh network. To remove this error an algorithm called as AODV routing algorithm is implemented. In this data is sent to the node which requires it and not to all the nodes in the network. The network persist coordinator and masters. Coordinator holds all the data. Master sends request to Coordinator that it requires data, then coordinator sends data to respected master. Masters can be termed as sensor. Coordinator to master follows shortest path. To prevent the route request buffers from growing indefinitely, each entry expires after a certain period of time, and then is removed. Furthermore, each node's buffer has a maximum size. If nodes are to be added beyond this maximum, then the oldest entries will be removed to make room.

1.4 Cryptography

The technique we are using here is Cryptography technique. The simplified meaning of cryptography is encryption. Encryption is the process of coding the information in such a way that its meaning is hidden. The reverse process of encryption is decryption. Encryption and Decryption uses a key. The coding is done in such a way that decryption is done only when proper key is known. Now a day's cryptography is not only encryption and decryption, it is developed to provide

1. Confidentiality: The prevention of unauthorized disclosure of information.
2. Integrity: The prevention of erroneous modification of information.
3. Availability: The prevention of unauthorized withholding of information or resources.
4. Authentication The process of verifying that users are who they claim to be when logging onto a system.
5. Authorization: The process of allowing only authorized user's access to sensitive information. Privacy ensures that the only the sender and intended. Recipient of an encrypted message can read the contents of the message that are transmitted from one place to another and cannot be understood by any intermediate parties that may have intercepted the data stream. Non-repudiation provides a method to guarantee that a party to a transaction cannot falsely claim that they did not participate in that transaction.

(1)The type of operations used for transforming plaintext to cipher text.
(2)The number of keys used.
(3)The way in which the plaintext is processed.

2. Comparison of the Results

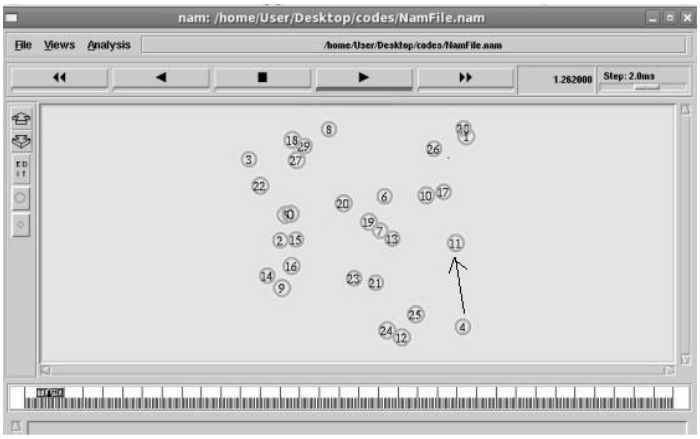

Fig -1: Network without application of algorithm

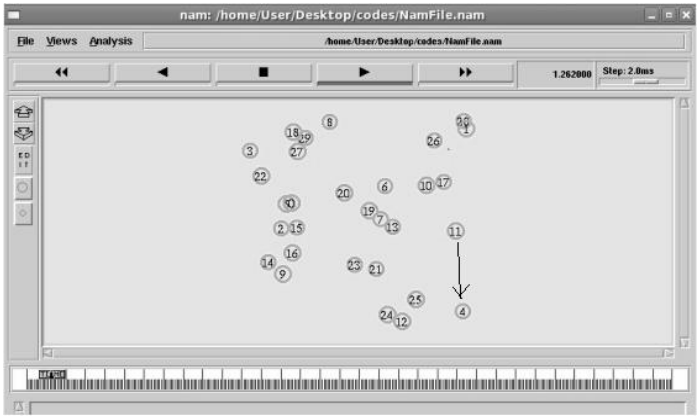

Fig -2: Master requesting Coordinator

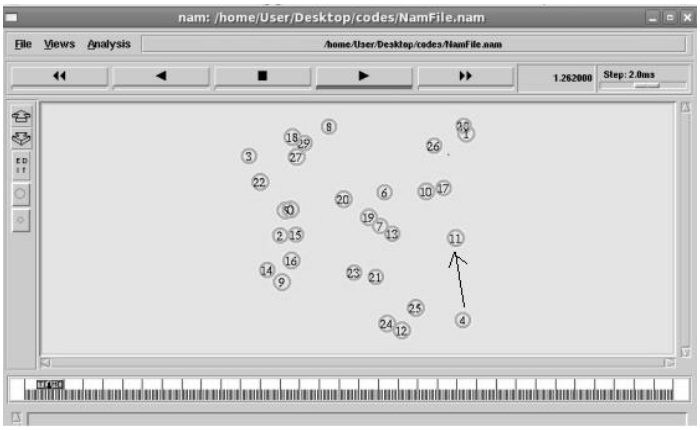

Fig -3: Coordinator sending data to master

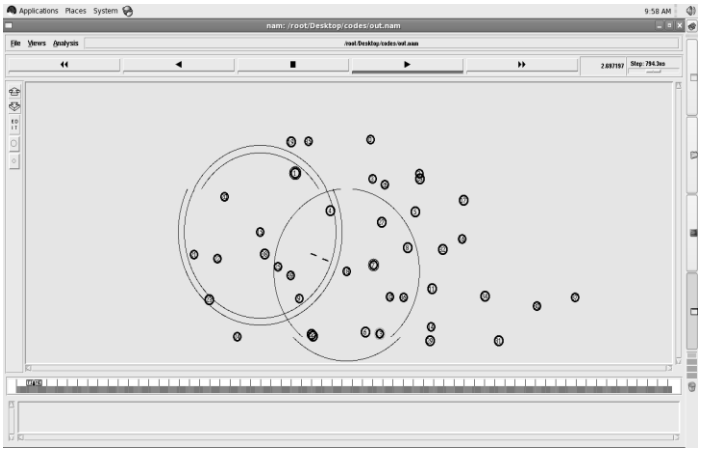

Fig -4: AODV network after removal of attack

Parameter	Normal value	Optimized value
Delay	3.7msec	3.5msec
Energy	550 joules	100 joules
PDR	100	100

In case of attack on the system and after removal of attack we get

Parameter	Normal AODV	With Attack	After removal of Attack
PDR	99.5	23.38	63.194
Delay (ms)	20.93	0	14.6

3. Conclusion

In this project very efficient and simple algorithm has been proposed for reducing overhead latency in wireless sensor network. Using this AODV algorithm the latency is successfully reduced.

In future we will try to increase the PDR after applying the algorithm to remove the attack. And try to reduce the delay. The evaluation parameters like energy, throughput will be studied. The other routing protocol will also be studied and will be checked the effect of attack on the other routing protocol.

In this paper performance of the normal AODV is studied, attacks are applied on the normal AODV because of the black hole attack the performance of the normal AODV gets degraded due to which the packet delivery ratio also get decreased and the delay get increased. A cryptographic technique is used to remove the black hole attack, in which the RC6 algorithm is applied on the network. Due to which the PDR get increased and the delay get increased.

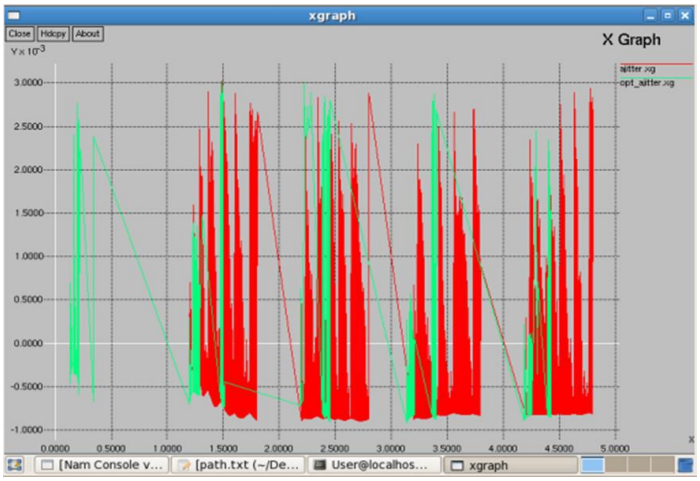

Fig -4: Graph between normal delay and optimized delay

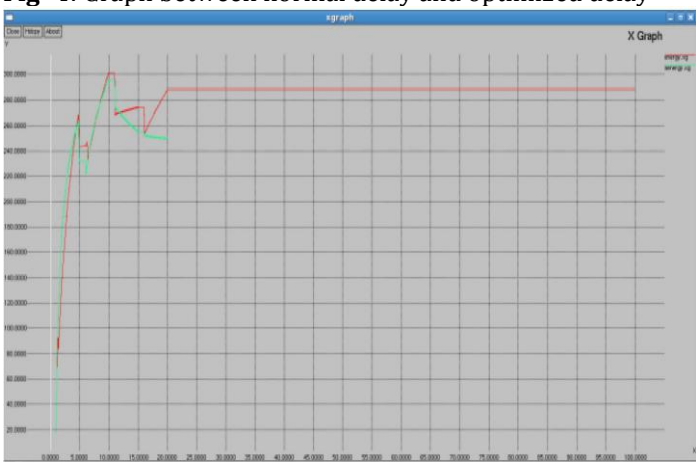

Fig -5: Graph between normal energy and optimized delay

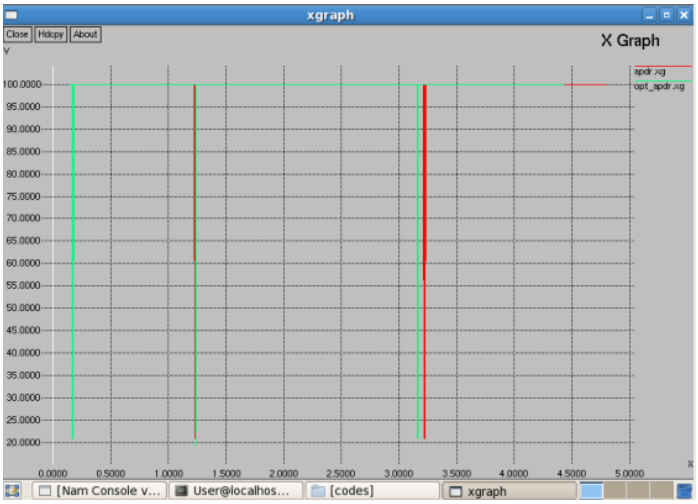

Fig -6: Graph between normal PDR and optimized PDR

ACKNOWLEDGEMENT

Author takes this opportunity to express our sincere and deep regards to our guides Prof. Mr. M. S Pawar sir, Prof. Y. Suryawanshi sir for their constant guidance and encouragement. We are grateful for their cooperation. We would like to thank all our concerned lecturers and friends who supported and helped us.

REFERENCES

[1] J. Song, J.-D. Ryoo, S. Kim, J. Kim, H. Kim, and P. Mah, "A dynamic GTS allocation algorithm in IEEE 802.15.4 for QoS guaranteed real-time applications," in Proc. IEEE Int. Symp. Consum. Electron., Jun. 2007,pp. 1-6.

[2] Seryvuth Tan, Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.

[3] Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathurl and Prashant Khurana, "A Modified AODV against single and collaborative Black Hole attacks in MANETs", 2013 27th International Conference on Advanced Information Networking and Applications Workshops.

[4] Haifeng Zheng, Shilin Xia, Xinbing Wang, Xiaohua Tian,"Energy and Latency Analysis for In-network Computation with Compressive Sensing in Wireless Sensor Networks",The 3151 annual IEEE International Conference.

[5] Morli Pandya, Ashish kr. Shrivastava, Rajiv Gandhi Proudyogiki Vishwavidyalaya "Improvising the Performance with Security of AODV Routing Protocol in MANETs" 2013 Nirma University International Conference on Engineering.

BIOGRAPHIES

Neha Arun Ingley
Assistant Professor,
Dept. of Electronics Engineering,
Yeshwantrao Chavan College of Engineering, Nagpur

Prachi Dhanraj Gawande
Assistant Professor,
Dept. of Electronics and Telecommunication Engineering,
Yeshwantrao Chavan College of Engineering, Nagpur