RESEARCH ARTICLE OPEN ACCESS

NEO WSN: Network Lifetime Enhancement with OSPFV3 Authentication Scheme in Wireless Sensor Networks

Hema M[1], Natchadalingam R[2]

[1] (ME-Dept of CSE (with specialization in Networks), PSN Engineering College, Tirunelveli, Tamilnadu, India)

[2] (Professor Dept of CSE, PSN Engineering College, Tirunelveli, Tamilnadu, India)

----------**********----------

Abstract

In Wireless Sensor Networks (WSN) Routing and Security are the main design issues for message delivery. Here we propose a new application-NEO WSN: Network Lifetime Enhancement with OSPFV3 Authentication Scheme that balance the entire sensor network energy consumption and thereby extend the sensor network lifetime. In our system Network Lifetime Enhancement with OSPFV3 Authentication Scheme for Security is proposed. The NEO Routing protocol provides shortest path for information routing and balance the energy using energy balance control parameter thereby growing the network lifetime. Then Open Shortest Path First version 3 IPSec ESP Encryption and authentication scheme provides security and integrity and confidentiality. Our theoretical analysis and NS2 simulation results demonstrate that the proposed protocol can provide an excellent tradeoff between routing efficiency, energy balance and can significantly extend the lifetime of the sensor networks in all scenarios. This method provides efficient routing and security for wireless sensor networks.

Keywords: **Routing, security, Energy efficiency, Energy Balance Parameter, Authentication, Simulation**

----------**********----------

1. INTRODUCTION

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as sound temperature, strain, etc. Routing is a very challenging design issue for WSNs. A routing protocol should not only ensure elevated message delivery ratio and low energy expenditure for message release, but also balance the entire sensor network energy utilization and thereby extend the sensor network lifespan. Security is another one challenging of design issue for WSNs. In particular, in the wireless sensor domain, anybody with an suitable wireless receiver can observe and intercept the sensor network communications. The adversaries may use expensive radio transceivers, powerful workstations and interact with the network from a distance since they are not restricted to using sensor network hardware. It is possible for the adversaries to perform jamming and routing traceback attacks.

Motivated by the fact that WSNs routing is often high energy based, we propose a

Network Lifetime Enhancement with OSPFV3 Authentication Scheme relying on flooding. NEO allows messages to be transmitted using two routing strategies, for message forwarding: shortest path message forwarding, secure message forwarding. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks.

NEO protocol has two major advantages: (i) It ensures balanced energy utilization of the entire sensor network so that the lifetime of the WSNs can be maximized. (ii) It reduces the packet loss. (iii)It prevents the malicious traffic jamming attacks during routing time in WSNs.

Our assistance of this paper can be summarized as follows: We propose a NEO WSN: Network Lifetime Enhancement with OSPFV3 Authentication Scheme in Wireless Sensor Networks. In this protocol, high energy based routing strategies can be applied to address the message delivery requirements. We devise a quantitative scheme to balance the energy consumption so that both the sensor network lifetime.

We develop theoretical formulas to estimate the number of routing hops in NEO under varying routing energy balance control and security requirements. We quantitatively analyze security of the proposed routing algorithm.

Our theoretical and simulation results both shows that the lifespan and the number of messages can be raised simultaneously. The rest of this paper is prepared as follows. In Section II, the related work is review The system model is presented in Section III. The future scheme is described in Section IV. In Section V, security analysis of the proposed scheme is conducted. Section VI provides performance analysis of the proposed scheme. We conclude in Section VII.

2. RELATED WORK

Routing is a challenging task in WSN's due to the limited resources. Geographic routing has been widely viewed as one of the most promising approaches for WSN's. Geographic routing protocols utilize the geographic location information to route data packets hop-by-hop from the source to the destination [4]. In [2], we developed criteria to quantitatively measure source-location information leakage for routing-based schemes through source-location disclosure index (SDI) and source-location space index (SSI). To the best of our knowledge, none of these schemes have considered privacy from a cost-aware perspective. The source chooses the immediate neighboring node to forward the message based on either the direction or the distance [13].

The delivery ratio can be improved if each node is aware of its 2-hop neighbors. In [5], discussed combining greedy and face routing to solve the local minimum problem. The basic idea is to set the local topology of the network as a planar graph, and then the relay nodes try to forward messages along one or possibly a sequence of adjacent faces toward the destination. Then [6] investigated the unbalanced energy consumption for uniformly deployed data-gathering sensor networks. In this paper, the network is divided into multiple corona zones and each node can perform data aggregation.

A localized zone-based routing scheme was proposed to balance energy consumption among nodes within each corona. As discussed in [12], dynamic routing is an effective method to minimize the probability of jamming. The adhoc routing algorithm distributes the routing paths in a large area based on our above analysis due to the random and independent routing selection strategy in each forwarding node. This

makes the likelihood for multiple messages to be routed to the sink node through the same routing path very low even for the smart jammers that have knowledge of the routing protocol.

In [8], [9], we developed a two-phase routing algorithm to provide both content confidentiality and source-location privacy. The message is first transmitted to a randomly selected intermediate node in the sensor domain before the message is being forwarded to a network mixing ring where the messages from different directions are mixed. Then the message is forwarded from the ring to the sink node.

The authors in [7] formulated the integrated design of route selection, traffic load allocation, and sleep scheduling to maximize the network lifetime. In addition, exposure of routing information presents significant security threats to sensor networks. By acquisition of the location and routing information, the adversaries may be able to trace back to the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design [8]–[9]. Jamming attacks have been extensively studied [11], [12].

The main idea is that the jammers try to interfere with normal communications between the legitimate communication parties in the link layer and/or physical layer. However, a jammer can perform attacks only when the jammer is on the message forwarding path. To solve this problem, directed walk, through either a sector-based or a hop-based approach, was proposed. Take the section-based directed walk, for example. The source node first randomly determines a direction that the message will be sent. This direction information is stored in the header of the message. Every forwarder on the random walk path will forward this message to a random neighbor in the same direction as the source node did so that the phantom source can be far away from the actual source. Unfortunately, once the message is captured on the random walk path, the adversaries will be able to get the direction information stored in the header of the message. Therefore, exposure of the direction information decreases the complexity for adversaries to trace back to the actual message source in the order of 2h [1].

In this paper, for the first time, we propose a Network Lifetime Enhancement with OSPFV3 Authentication Scheme that can address energy balance and routing security concurrently in WSN's. In NEO protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design tradeoff between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries. Our extensive NS2 simulation results show that NEO protocol can provide excellent energy balance and routing security. It is also demonstrated that the proposed secure routing can increase the message delivery ratio due to reduced dead ends and loops in message forward.

3. MODELS AND ASSUMPTIONS

3.1. The System Model

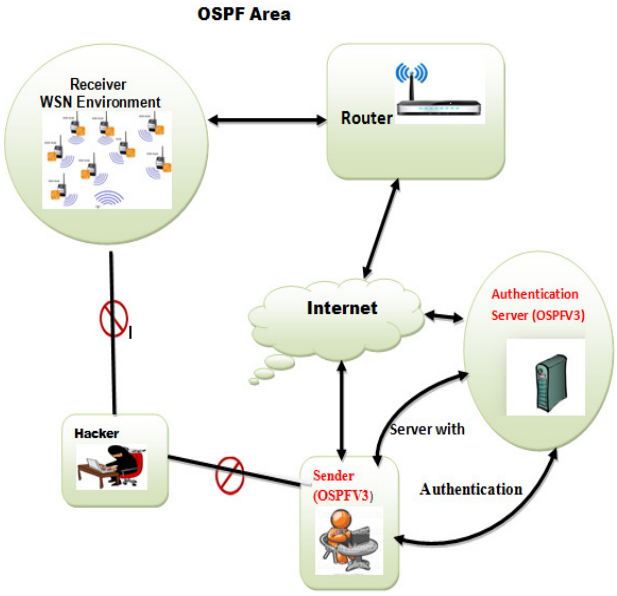

Fig 1: System Architecture Design

3.2. Design Goals

Our design purpose can be summarized as follows:

- To maximize the sensor network lifespan, we ensure that the energy utilization of all sensor grids are balanced.
- The Hacker should not be able to get the source location information.
- Only the sink node is able to identify the source location through the message received because of the secured authentication..
- It is Provide high Secure Routing using in Authentication Scheme.
- Its ensure security, data integrity and confidentiality.

3.3 Overview of Proposed Scheme

In our scheme, the network is evenly divided into small grids. Each grid has a relative location based on the grid information. The node in each grid with the highest energy level is selected as the head node for message forwarding. In addition, each node in the grid will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighboring grids. The information maintained by each sensor node will be updated periodically.

While maximizing message source location privacy and minimizing traffic jamming for communications between the sources and the destination nodes, we can optimize the sensor network lifetime through balanced energy consumption throughout the sensor network. In addition, through the maintained energy levels of its adjacent neighboring grids, it can be used to detect and filter out the compromised nodes for active routing selection and secure authentication.

4. THE PROPOSED NEO-WSN SCHEME

For node A, denote the set of its immediate adjacent neighboring grids as NA and the remaining energy of grid i as Eri, iєNA. For this purpose, we introduce a parameter α€ [0, 1] to enforce the degree of the energy balance control (EBC).We define the candidate set for the next hop node as NαA ={iєNA|Eri ≥αEα(A)} based on the EBC α.

Algorithm: Node A finds the next hop routing grid based on the EBC α€ [0, 1]

1: Calculate the average remaining energy of the adjacent neighboring grids:

Eα(A) = 1/(|NA|) * (∑i€ NA Eri)

2: Establish the candidate grids for the next routing hop:

$$N\alpha A=\{i \epsilon NA | Eri \geq \alpha E\alpha(A)\}$$

3: Send the message to the grid in the NA that is closest to the sink node based on its relative location.

Steps Involved are

Compute the average remaining energy of the closest neighboring nodes

$$E\alpha(A) = 1/(|NA|) * (\sum i \epsilon NA\ Eri) \quad (1)$$

Establish the candidate grids for the next routing node

$$N\alpha A=\{i \epsilon NA | Eri \geq \alpha E\alpha(A)\} \quad (2)$$

The system implementation involves the following modules:

1. Cluster formation

This module creates group of nodes including sender and sink node.

2. Encryption and Authentication

Information is encrypted and adding the authentication header using OSPFV3 Protocol

3. Energy Efficient Routing

Routing the encrypted information with NEO protocol

4. Message Forwarding and Decryption

Forwarding the information for decryption and Sending to the sink node.

5. Security analysis

The security scheme that has been implemented here is summarized below:

OSPFv3 IPSec ESP Encryption and Authentication (OSPFv3).It runs on IPv6. OSPFv3 requires the IPv6 encapsulating security payload (ESP) header or IPv6 authentication header to ensure truthfulness, authentication, and privacy of routing interactions. IPv6 ESP extension headers can be used to provide authentication and privacy to OSPFv3.

Steps involved are:

- Enables confidential EXEC mode.
- Enters global configuration mode.
- Enables OSPFv3 router design mode.
- Enables authentication for implicit links in an OSPFv3 area.
- Enables encryption for implicit links in an OSPFv3 area

6. PERFORMANCE EVALUATION AND SIMULATION RESULTS

6.1. Simulation Environment

Our model is based on the MAC layer of the IEEE 802.11b, which is included in the NS2.The transport protocol is User Datagram Protocol (UDP). Traffic sources are Constant Bit Rate (CBR). The number of nodes is equally distributed over the entire network.
In Figure 2 show that the simulation result of the proposed scheme

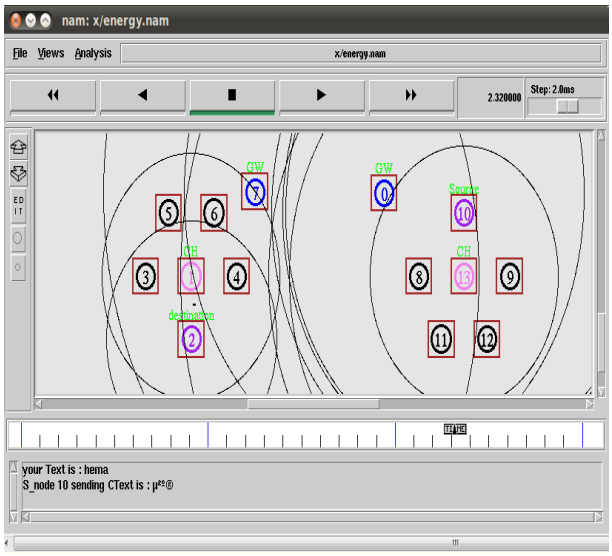

Fig 2: Network Simulation for proposed scheme

6.2Performance Analysis

6.2.1 Message Loss

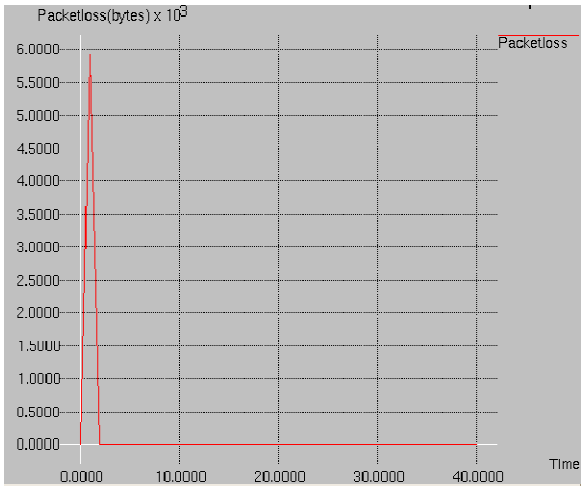

Fig 3: Message loss with traffic load

Figure 3 shows the relationship between the message loss and the traffic load. Here the traffic load is denoted by the number of nodes associated with the Router. Clearly we can observe that the message loss increases with the increase in traffic load but using our scheme, the lowest message loss is yielded.

6.2.2 Throughput

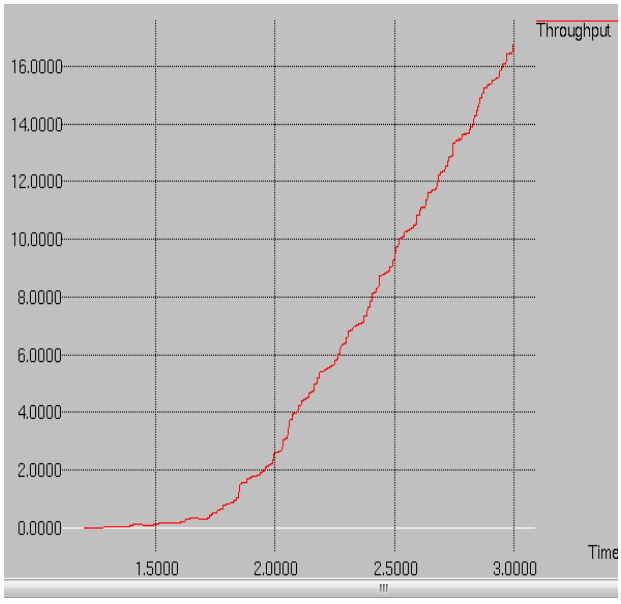

Fig 4: Throughput with time interval

Figure 4 shows the correlation between the throughput and the time interval. As the time increases the system attains the maximum throughput value.

6.2.3 Energy Efficiency

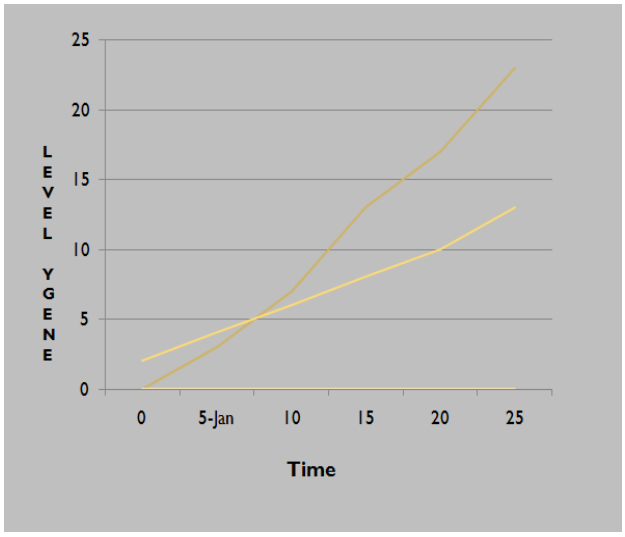

Fig 5: Energy level with time interval

Figure 5 shows the correlation between the energy level and the time interval. As the time increases the system attains the maximum energy level.

7. CONCLUSIONS AND FUTURE WORK

In this paper, a Network Lifetime Enhancement with OSPFV3 Authentication Scheme in WSNs is presented to balance the energy utilization and increase network life span. NEO has the flexibility to support multiple routing strategies in message forwarding to extend the lifetime while implementing the routing security. For security purpose, we have OSPF in a number of key areas but have held back by its proprietary nature and costs. OSPF has advantages in large networks where its hierarchical nature increases scalability. Both theoretical analysis and simulation results show that NEO has an excellent routing performance in terms of energy

balance and routing path distribution for routing path security.

In our future work, we will expand our idea about NEO routing with congestion control mechanism to decrease the packet loss and test it by simulation.

REFERENCES

[1] Di Tang,Tongtong Li,Jian Ren,Jie Wu "Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks",IEEE Transactions on Parallel and Distributed Systems DOI 0.1109/TPDS.2014.2318296,JULY 2014.

[2] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems.

[3] Alex Hinds, AnthonyAtojoko,and Shao Ying Zhu "Evaluation of OSPF and EIGRPRouting Protocols for IPv6 "IEEE Transactions On Parallel And Distributed Systems Vol. 2, August 2013.

[4] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in IEEE INFOCOM 2012 Mini-Conference, Orlando, USA March 25-30, 2012 2012.

[5] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," Mobile Computing, IEEE Transactions on, vol. 9, no. 4, pp. 582–595, April 2010.

[6] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks, "Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.

[7] F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 9, no. 7, pp. 2258 2267, July 2010

[8] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proceedings of IEEE SECON 2009, Rome., June 22-26, 2009.

[9] "Source location privacy through dynamic routing in wireless sensor networks," in Proceedings of IEEE INFOCOM 2010, San Diego, USA. March 15-19, 2010.

[10] Information About OSPFv3 IPSec ESP Encryption and Authentication, IP Routing: OSPF Configuration Guide, Cisco IOS Release 15SY10.

[11] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," IEEE Network, vol. 20, no. 3, pp. 41–47, 2006.

[12] Pathan, H.-W. Lee, and C. seon Hong, "Security in wireless sensor networks: issues and challenges," in The 8th International Conference on Advanced Communication Technology (ICACT), vol. 2, 2006, pp. 6 :pp.–1048

[13] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks,"UCLA Computer Science Department Technical Report, UCLACSD, May 2001.

[14] H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor

Networks," Computer Networks,vol. 53, no. 9, pp. 1512-1529, 2009.

[15] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on"perturbation polynomials"." Cryptology ePrint Archive, Report 2009/098, 2009. http://eprint.iacr.org/