A Novel Approach for Protecting Location Privacy in Wireless Sensor Networks

Bhargavi Badiginchala
Master of Computer Applications
Narayana Engineering College
Nellore,(JNTUA)
Nellore,India
badginchalabhargavi@gmail.com

Chandana Musunuru
Master of Computer Applicatios
Narayana Enginering College,
Nellore(JNTUA)
Nellore,India
chandanamusunuru1998@gmail.com

Lakshmi Prasanna Thommandra
M.C.A,M.Tech
Narayana Engineering College,
Nellore(JNTUA)
Nellore,India
lakshmiprasanna54@gmail.com

Suresh Pathipatti
Master of Computer Applicatios
Narayana Engineering College
Nellore,India
suresh.it@narayanagroup.com

ABSTRACT :With the recent developments of Wireless Sensor Networks (WSNs), computing and communication have experienced huge advancement. Meanwhile, security has not received the same attention to go along with such developments. In this project, i focus on the source location privacy problem in WSNs, a hot research topic in security, and propose A NOVEL APPROACH FOR PROTECTING LOCATION PRIVACY (NAPLP) IN WIRELESS SENSOR NETWORKS. A more powerful adversary, which can use Hidden Markov Model (HMM) to estimate the state of the source. To cope with this type of adversary, phantom nodes and fake sources, which are responsible to mimic the behavior of the source, are utilized to diversify the routing path. Then, the weight of each node is calculated as a criteria to select the next-hop candidate. In addition, two transmission nodes are designed to transmit real packets. The simulation results demonstrate that the proposed NAPLP scheme improves the safety time without compromising the energy consumption.

1. INTRODUCTION

Security of WSNs involves many aspects, such as data privacy and location privacy. Data privacy can be protected by encryption algorithms while location privacy cannot be protected to the extreme. Due to the time correlation in data transmission between two nodes, the adversary can infer location information through analysis

Security has not received the same attention to go along with such developments. In this project, i focus on the source location privacy problem in WSNs, a hot research topic in security, and propose A Novel Approach for protecting location privacy scheme (NAPLP) for WSNs. A more powerful adversary, which can use Hidden Markov Model (HMM) to estimate the state of the source. To cope with this type of adversary, phantom nodes and fake sources, which are responsible to mimic the behaviour of the source, are utilized to diversify the routing path the proposed NAPLP scheme improves the safety time without compromising the energy consumption.

2. RELATED WORK:

Wireless Sensor Networks (WSNs) consist of numerous sensor nodes and protocols, which is the basis of service like information authentication, event awareness, and node charging. These nodes play the role of microcomputer and are distributed in various environments. There are a lot of data transmissions and communication behaviors between nodes. So, it is essential to preserve the security. Security of WSNs involves many aspects, such as data privacy and location privacy. Data privacy can be protected by encryption algorithms while location privacy cannot be protected to the extreme.

Due to the time correlation in data transmission between two nodes, the adversary can infer location information through analysis. From a time correlation perspective, location privacy consists of the source location privacy and the sink location privacy. Given the importance of the source, in this project, i focus on the source location privacy, which is an emerging research topic in the field of security. There are many techniques, like secure routing, fake sources, phantom nodes, fake cloud, and cluster, that can be applied to protect the source location privacy. We propose A Novel Approach for protecting location privacy scheme (NAPLP), which adopts phantom nodes and fake sources for the reason that these two techniques can diversify the routing path.

Disadvantage of Existing System

The system is less effective due to lack of source location privacy.

The system has only detection techniques and no protection techniques.

3 .PROPOSED SYSTEM

NAPLP has exhibited a better performance than two other recent schemes in our simulations with regard to increasing the safety time while balancing the energy consumption. The main contributions of this paper are:

Both phantom nodes and fake sources are integrated into the proposed NAPLP, which enhance the source location privacy.

A more powerful local adversary, which can use Hidden Markov Model to estimate the state of the source, is taken into consideration.

Two data transmission modes are designed based on the distance between the source and the sink, which further enhance the source location privacy.

4. WORK FLOW PROCESS

1. Service provider:

In this module, the service provider will browse the data file, initialize the router nodes, for security purpose service provider encrypts the data file and then sends to the particular receivers (A, B, C, D…). Service provider will send their data file to router and router will select smallest distance path and send to particular receive

2. Router

The Router manages a multiple nodes to provide data storage service. In router n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and routing path details. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then flow will be send to IDS manager and router will connect to another node and send to particular receiver.

3. IDS Manager

In this module, the IDS Manager detects introducer and stores the introducer details. In a router any type of attacker (Active or passive attacker) is found then details will send to IDS manager. And IDS Manager will detect the attacker type (Active attacker or passive attacker), and response will send to the router. And also inside the IDS Manager we can view the attacker details with their tags such as attacker type, attacked node name, time and date.

4. Receiver (End User)

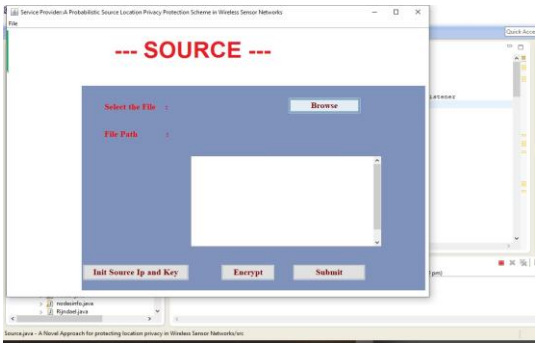
In this module, the receiver can receive the data file from the router. Service provider will send data file to router and router will accept the data and send to particular receiver (A, B, C, D, E and F). The receivers receive the file in decrypted format by without changing the File Contents. Users may receive particular data files within the network only.

5.Attacker

In this module, there are a two types of attacker is present one is active attacker and passive attacker. Active attacker is one who is injecting malicious data to the corresponding node and also passive attacker will change the destination IP of the particular node. After attacking a node we can view attacked nodes inside router.

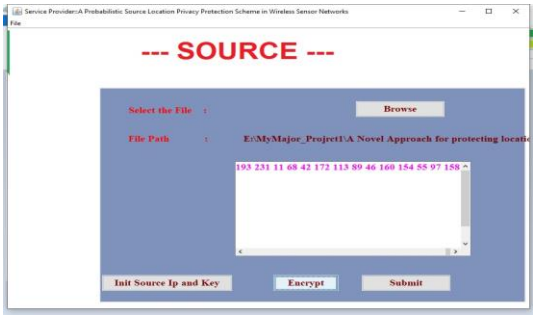
5. EXPERIMENTAL RESULTS

1. Home page



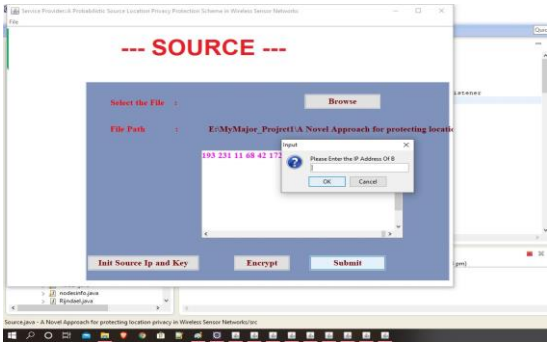
The above screen shows the Selection of file process

2. File selection



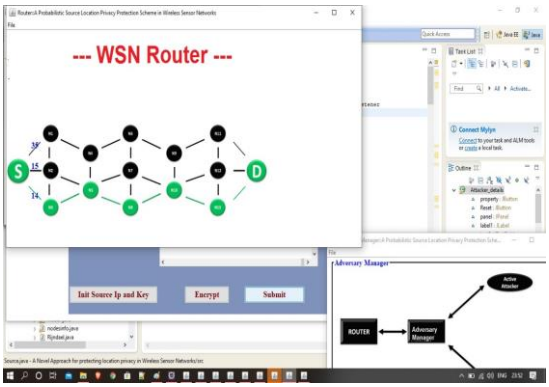
Selecting and allocating path in path menu

3. Entering of IP Address



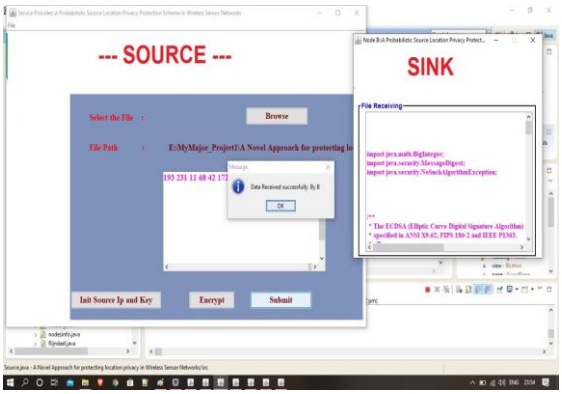
Enter the IP Address in specified path

4. Source to Destination Approach



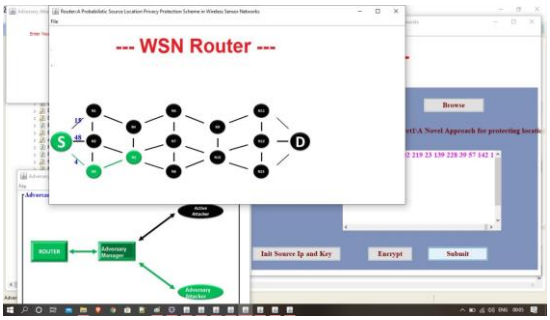
The above screen shows Path formed from Source to Destination

5. Reached to Destination



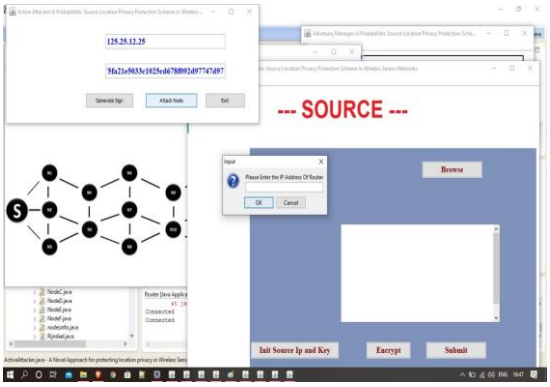
The above screen shows reached to the destination

6. Selecting the shortest Path Route



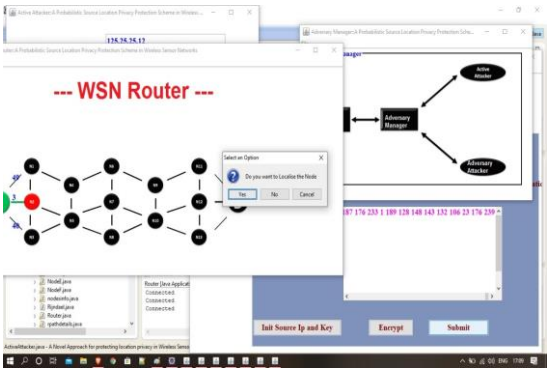
This screen shows the selection of shortest path

7. Entering the Router IP Address



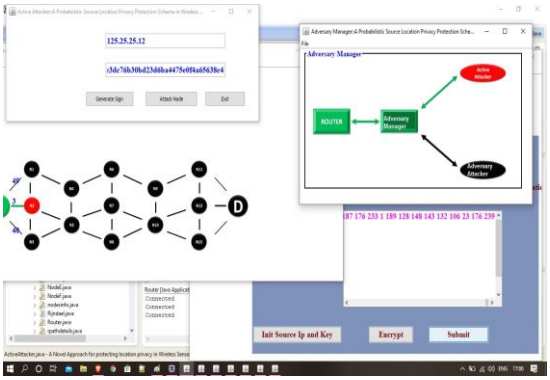
This screen explains the source requesting destination IPAddress

8. Selecting the another path

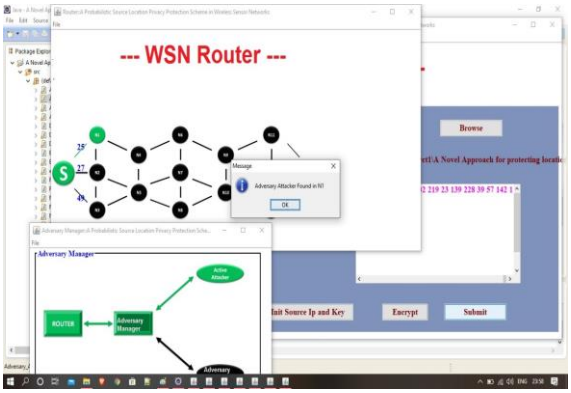


The above screen explains the selection of another path due to attacker

9. Adversary manger selected the another path

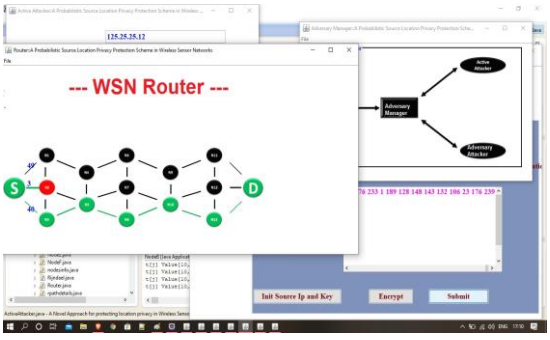


10.Adversary Manager changing the Route



The above screen explains the adversary manager identified the attacker in the source path

11. Reached to Destination



The above screen shows after detecting the attack source is redirected to another path

6. CONCLUSION

Studying security in WSNs became increasingly important during the last decade. The source location privacy, a research hotspot in security, and proposed A Novel Approach for protecting location privacy scheme based on WSNs. A powerful adversary which utilizes Hidden Markov Model (HMM) is considered in this study. To cope with it, phantom nodes, fake sources, and weight are adopted to change the packets' transmission directions. Considering the distance between the source and the sink, two types of routing modes are designed. Compared with Dynamic SPR and SLPE, the simulation results demonstrate that the proposed NAPLP achieves a high safety time and balances the energy consumption of each node.

7. FUTURE ENHANCEMENT

Any project that has been already developed can always be improved further for better efficiency, better performance, easy understanding and important of all satisfy user to a higher extent. Future studies will concentrate on protecting the source location by reducing the adversary's monitoring probability and secure communication among nodes.

References:

H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular

ad hoc networks: a survey," Wireless Communications and Mobile

Computing, vol. 16, no. 6, pp. 643-655, Apr. 2016.

W. Chen, M. Zhang, G. Hu, X. Tang, and A. Sangaiah, "Constrained

Random Routing Mechanism for Source Privacy Protection in WSNs,"

IEEE Access, vol. 5, pp. 23171-23181, Sept. 2017.

A. Proa~no, L. Lazos, and M. Krunz, "Traffic Decorrelation Techniques

for Countering a Global Eavesdropper in WSNs," IEEE Transactions on

Mobile Computing, vol. 16, no. 3, pp. 857-871, Mar. 2017.

R. Manjula and D. Raja, "A novel source location privacy preservation

technique to achieve enhanced privacy and network lifetime in WSNs,"

Pervasive and Mobile Computing, vol. 44, pp. 58-73, Feb. 2018.

N. Wang, J. Fu, J. Zeng, and B. Bhargava, "Source-location privacy full

protection in wireless sensor networks," Information Sciences, vol. 444,

pp. 105-121, May 2018.

G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: A kmeans

Cluster-Based Location Privacy Protection Scheme in WSNs for

IoT," IEEE Wireless Communications Magazine, vol. 25, no. 6, pp. 84-90,