www.ijiarec.com

DEC 2013

International Journal of Intellectual Advancements and Research in Engineering Computations

ENERGY CONSUMPTION AND LOCALITY OF SENSOR NETWORKS

[*1]Mr. S.Aravinth, [2]Mr. N.M.K.Ramalingam Sakthivelan,M.E.,

ABSTRACT

Wireless sensor networks (WSNs) are used in many areas for critical infrastructure monitoring and information collection. For WSNs, SLP service is further complicated by the nature that the sensor nodes generally consist of low-cost and low-power radio devices. Computationally intensive cryptographic algorithms (such as public-key cryptosystems), and large scale broadcasting-based protocols may not be suitable. Propose criteria to quantitatively measure source-location information leakage in routing-based SLP protection schemes for WSNs. Through this model, identify the vulnerabilities of SLP protection schemes. Propose a scheme to provide SLP through routing to a randomly selected intermediate node (RSIN) and a network mixing ring (NMR). The security analysis, based on the proposed criteria, shows that the proposed scheme can provide excellent SLP. The message will send securely. The adversaries cannot able to identify the source location. The adversaries cannot make any interruption to the message because of the secure algorithms. The comprehensive simulation results demonstrate that the proposed scheme is very efficient and can achieve a high message delivery ratio. It can be used in many practical applications.

Index terms: Light key cryptosystems,randomly selected intermediate node, Network mixing ring, Source location privacy.

I INTRODUCTION

Wireless sensor networks (WSNs) have been envisioned as a technology that has a great potential to be widely used in both military and civilian applications. Sensor networks rely on wireless communication, which is by nature a broadcast medium and is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In the wireless sensor domain, anybody with an appropriate wireless receiver can monitor 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 identify the message source or even identify the source location, even if strong data encryption is utilized. Source-location privacy (SLP) is an important security issue. Lack of SLP can expose significant information about the traffic carried on the network and the physical world entities. While confidentiality of the message can be ensured through content encryption, it is much more difficult to adequately address the SLP. Preserving SLP is even more challenging in WSNs since the sensor nodes consist of only low-cost and low-power radio devices, and are designed to operate unattended for long periods of time. Battery recharging or replacement may be infeasible or impossible. Computationally intensive cryptographic algorithms, such as public-key cryptosystems, and large scale broadcasting based protocols, are not suitable for WSNs.To optimize the sensor nodes for the limited node capabilities and the application specific nature of the WSNs, traditionally, security requirements were largely ignored. This leaves WSNs vulnerable to network security attacks. In the worst case, adversaries may be able to undetectably take control of some wireless sensor nodes, compromise the cryptographic keys, and reprogram the wireless sensor nodes. In this paper, first propose some

Author for Correspondence:

[*1]Mr.S.Aravinth, PG Scholar, Department of CSE, Sri Krishna Engineering College Panapakam, Chennai-301, India.
E-mail: cool88boy@gmail.com

[2]Mr.N.M.K.Ramalingam Sakthivelan, M.E., Asso.Professor Department of CSE, Sri Krishna Engineering College, Panapakam, Chennai-301, India.

criteria to quantitatively measure source-location information leakage for routing-based SLP schemes. It is easy to identify security vulnerabilities of some exiting SLP schemes.A scheme is proposed that can provide both content confidentiality and SLP through a two-phase routing. In the first routing phase, the message source randomly selects an intermediate node in the sensor domain and then transmits the message to the randomly selected intermediate node (RSIN). This phase provides SLP with a high local degree. In the second routing phase, the messages will be routed to a ring node where the messages will be blended through a network mixing ring (NMR). The proposed scheme is very efficient and can achieve a high message delivery ratio. It can be used in many practical applications.

The major contributions of this paper can be summarized

- To develop a model to quantitatively measure source-location information leakage for routing based SLP schemes.
- Identify three criteria to measure source-location information leakage for routing-based schemes.
- Propose a two-phase routing scheme to protect routing-based source-location information.
- To provide extensive simulation results using ns-2 to demonstrate the efficiency of proposed scheme.

II PROBLEM AND ANALYSIS

In the past two decades, originated largely from Chaum's mixnet a number of protocols have been proposed to provide SLP. The mixnet family protocols use a set of "mix" servers that blend the received packets so that the communication source (including the sender and the recipient) becomes ambiguous. They rely on the statistical properties of background traffic, also referred to as cover traffic, to achieve the desired anonymity. However, these schemes all require public-key cryptosystems and are not suitable for WSNs. Broadcasting-based schemes provide SLP by mixing the valid messages with the dummy messages so that they become indistinguishable to the adversaries. In a practical situation, the dummy messages can be significantly more than the valid messages. It consumes a significant amount of the limited energy, but also increases network collisions and decreases the packet delivery ratio. Therefore, these schemes are not quite suitable for large sensor networks. Providing SLP through dynamic routing is one of the most feasible approaches in WSNs. The main idea is to prevent the adversaries from tracing back to the source location through traffic monitoring and analysis. A representative example of a routing based protocol is the phantom routing protocol, which involves two phases: a random walk phase and a subsequent flooding/single path routing phase. In the random walking phase, the message from the actual source will be routed to a phantom source along a random path or a designed directed path. The phantom source is expected to be far away from the actual source, which will make the actual source's location hard to be traced back by the adversaries. However, theoretical analysis shows that if the message is routed h hops randomly, it is highly possible that the distance between the phantom source and the actual source is within h=5. 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 deterrmines 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 traceback to the actual message source in the order of 2h.

Network models and design goals

SLP is a key security requirement for military and many civilian applications. In the asset monitoring model, WSNs can be used to monitor the activities or presence of animals in a wild animal habitat. However, the information should be kept unavailable to illegal hunters. In military intelligence networks, to protect the message source, both the message source and the routing path have to be protected from adversarial attacks. Introduce the system model and adversarial model in this section to capture the relevant features of

WSNs and the potential adversaries in SLP applications. Michael G.Reed, Paul F Syverson, and D. Goldschlag says, that onion Routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and trac analysis. Onion routing's anonymous connections are bidirectional and near real time, and can be used anywhere a socket connection can be used. Any identifying information must be in the data stream carried over an anonymous connection. An onion is a data structure that is treated as the destination address by onion routers. Thus, it is used to establish an anonymous connection. Onions themselves appear differently to each onion router as well as to network observers. The same goes for data carried over the connections they establish. Proxy aware applications, such as web browsing and e-mail, require no modification to use onion routing, and do so through a series of proxies. This describes anonymous connections and their implementation using onion routing. It also describes several application proxies for onion routing, as well as configurations of onion routing networks. Michael k.Reiter and Aviel D.Rubin introduce a system called Crowds for protecting users' anonymity on the world-wide-web. Crowds, named for the notion of blending into a crowd", operates by grouping users into a large and geographically diverse group (crowd) that collectively issues requests on behalf of its members. Web servers are unable to learn the true source of a request because it is equally likely to have originated from any member of the crowd, and even collaborating crowd members cannot distinguish the originator of a request from a member who is merely forwarding the request on behalf of another. Describe the design, implementation, security, performance, and scalability of the system. The security analysis introduces degrees of anonymity as an important tool for describing and proving anonymity properties. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk explained the most notable challenges threatening the successful deployment of sensor systems is privacy. Although many privacy-related issues can be addressed by security mechanisms, one sensor network privacy issue that cannot be adequately addressed by network security is source-location privacy. Adversaries may use RF localization techniques to perform hop-by-hop trace back to the source sensor's location. This provides a formal model for the source-location privacy problem in sensor networks and examines the privacy characteristics of different sensor routing protocols. Examine two popular classes of routing protocols: the class of flooding protocols, and the class of routing protocols involving only a single path from the source to the sink. While investigating the privacy performance of routing protocols, the tradeoffs between location-privacy and energy consumption and the current protocols cannot provide efficient source-location privacy while maintaining desirable system performance. In order to provide efficient and private sensor communications, It devised new techniques to enhance source-location privacy. One of the strategies, a technique that have called phantom routing, has proven flexible and capable of protecting the source's location, while not incurring a noticeable increase in energy overhead. Further, examined the effect of source mobility on location privacy,showed that, even with the natural privacy amplification resulting from source mobility, the phantom routing techniques yield improved source-location privacy relative to other routing methods.

III SOLUTION AND MECHANISM

1) First propose some criteria to quantitatively measure source-location information leakage for routing-based SLP schemes.

2) Propose a scheme that can provide both content confidentiality and SLP through a two-phase routing.

3) In the first routing phase, the message source randomly selects an intermediate node in the sensor domain and then transmits the message to the randomly selected intermediate node (RSIN). This phase provides SLP with a high local degree.

4) In the second routing phase, the messages will be routed to a ring node where the messages will be blended through a network mixing ring (NMR). By integrating the NMR, can dramatically decrease the local degree and increase the SLP.

To prevent the adversaries from getting any useful source-location information through correlation based source identification, a dynamic ID proposed for each message. Then, introduce a two-phase routing

protocol to provide SLP and content confidentiality. In the first phase, the source node routes the messages to a ring node through a single randomly selected intermediate node (RSIN) in the sensor domain before the message is routed to the mixing ring. Although this phase can provide a good SDI, the local degree is still large. In the second phase, the message from the first phase will be forwarded to the network mixing ring (NMR). The combination of these two phases guarantees the local degree to be small.The network is evenly divided into small grids. Assume that the sensor nodes in each grid are all within the direct communication range of each other. In each grid, the header node coordinates the communication with other header nodes nearby. The whole network is fully connected through the multihop communications.After the formation of all the grids, a large ring is generated in the sensor network to provide a network-level traffic mix. This ring is called the mixing ring. The mixing ring is composed of multiple header nodes. These header nodes are called as ring nodes. The ring nodes are further divided into relay ring nodes and normal ring nodes. The messages transmitted in the mixing ring are referred to as vehicle messages. Vehicle messages will be transmitted in the ring in a clockwise direction, called ring direction. Only relay ring nodes can generate vehicle messages. The grids containing ring nodes as ring grids. Correspondingly, the grids without ring nodes are called normal grids. The sensor nodes in normal grids are defined as normal nodes.The messages sent by the normal nodes are referred to as messages. When a normal node has a message to transmit, the message will first be sent to the header node in that grid.The header node will then forward this message to a randomly selected intermediate node before it is forwarded to a ring node. The ring transmission provides a networklevel traffic mix. The detailed description of the proposed two-phase routing will be described in the subsequent sections.

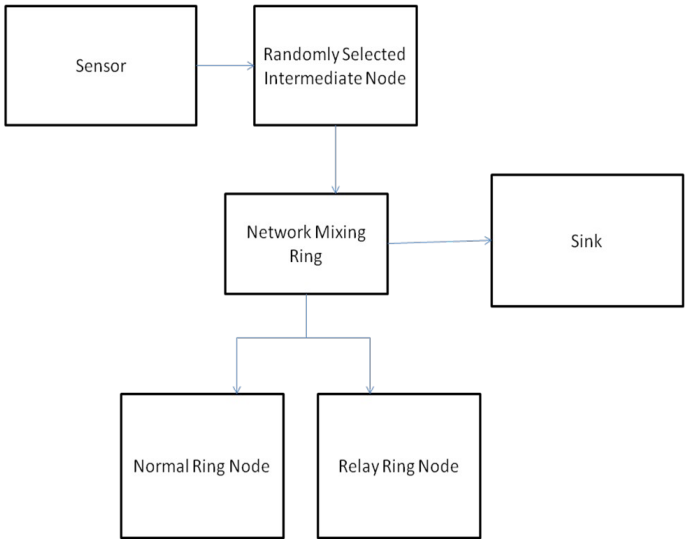

Fig 3.1: System architecture

Modules

- Key Management
- Randomly Selected Intermediate Node
- Network Mixing Ring
- Sink

KEY MANAGEMENT

Two kinds of keys in the scheme:

- Grid-key: the key shared between grid G and the SINK node.
- Ring-key: the key shared between ring grid A and ring grid B.

The grid-keys are used to provide message content confidentiality. When the i th normal grid has a message m to transmit, the message is first encrypted

using the grid key, then its dynamic ID j is prefixed to the encrypted message. Will be transmitted from the source node to the SINK node, the cipher text of m, encrypted using the secret key shared between the ith grid with dynamic ID and the SINK node.

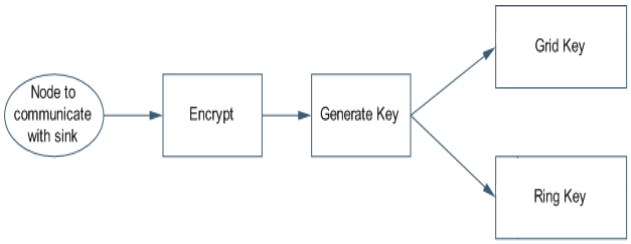

Fig 3.2: Key Mamagement Approach

Routing to a single intermediate node

As described before, phantom routing has no control over the phantom source without leaking significant side information. To solve this problem, in the proposed protocol, the message source first randomly selects an intermediate node at the sensor domain based on the relative location of the sensor node. The intermediate node is expected to be far away from the actual source node so that it is difficult for the adversaries to get the information of the actual source node from the intermediate node selected. Since assume that each sensor node only has knowledge of its adjacent nodes. The source node has no accurate information of the sensor nodes more than one hop away. In particular, the randomly selected intermediate node may not even exist. However, the relative location can guarantee that the message will be forwarded to the area of the intermediate node. The last node in the routing path adjacent to the intermediate node should be able to tell whether such a randomly selected intermediate node exists or not. In the case that such a node does not exist, this node will become the intermediate node. The intermediate node then routes the received message to a ring node.

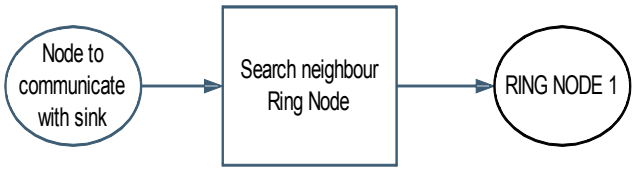

Fig 3.3: RSIN Approach

Network mixing ring (NMR)

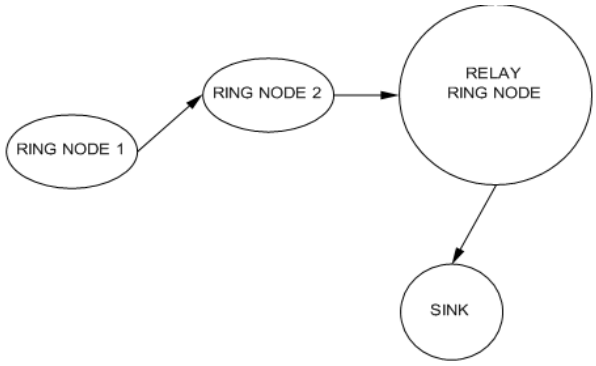

Fig 3.4: Architecture of NMR

In the mixing ring, each ring node can route messages toward its successor in the ring direction, which is the next hop node in a clockwise direction. The message can hop along the ring direction for a random number of hops before it is transmitted to the SINK node. This routing process provides SLP that resembles the airport terminal transportation system. In the mixing ring, only the relay ring nodes can initiate the vehicle messages starting with dummy messages, and deliver the vehicle messages to the SINK node. The normal ring nodes can store and forward messages received from the normal node to its successor ring node. The relay ring nodes can be either more powerful than or the same as the normal ring nodes.

In this scheme, the message source analysis, the message transmission in the ring is encrypted. Each ring node shares a secret key with its predecessor ring node and a secret key with its successor ring node. When an encryption algorithm is used, it is computationally infeasible for the adversary to find the correlation between the input and output of each node. The vehicle message should be sent at a rate which can ensure that all the messages are embedded in vehicle messages and forwarded to the SINK with minimum delay. Apparently, the energy drainage for the relay ring nodes will be faster than the normal ring nodes. On receiving a message, the SINK node identifies the source grid and decrypts the message to recover.

Sink

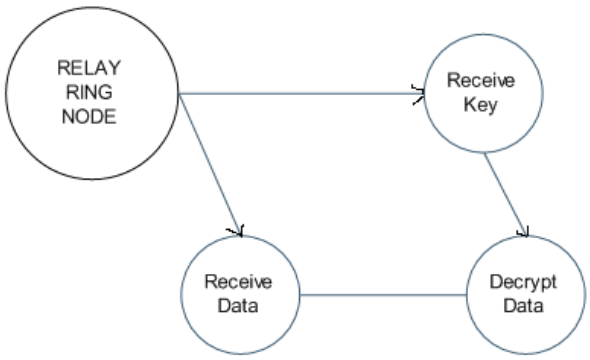

Fig 3.5: Architecture of Sink

To achieve a robust behavior of the ASM during matching, all outliers present must be rejected. In addition, it utilizes as many inliers as possible to achieve a good match between image and model. This has several implications for the selection of parameters for the RASM matching algorithm.

IV CONCLUSION

SLP is critical to the successful deployment of WSNs for many applications. In this paper, propose some criteria to quantitatively measure SLP for routing-based schemes. Based on these criteria, propose a scheme that can achieve SLP in WSNs through a two-phase routing: routing to a single RSIN and routing through the NMR. The optimal location for the mixing ring is also derived. The proposed scheme provides provable local SLP and global SLP. Simulation results demonstrate that the proposed scheme can achieve very good performance in energy consumption and message delivery latency, while assuring a high message delivery ratio.

REFERENCE

[1]. D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” Comm. the ACM, vol. 24, pp. 84-90, Feb.1981.

[2]. H. Wang, B. Sheng, and Q. Li, “Privacy-Aware Routing in Sensor Networks,” Computer Networks, vol. 53, no. 9, pp. 1512-1529, 2009.

[3]. M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Selected Areas in Comm., vol. 16, no. 4, pp. 482-494, May 1998.

[4]. M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transaction,"ACM Trans. Information and System Security, vol. 1, no. 1,pp. 66-92, 1998.

[5]. M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM '08, pp. 51-55, Apr. 2008.

[6]. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS '05), pp. 599- 608, June 2005.

[7]. Y. Li, L. Lightfoot, and J. Ren, "Routing-Based Source-Location Privacy Protection in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Electro/Information Technology (EIT '09), June 2009.