IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.
www.ijiset.com
ISSN 2348 - 7968

LOCATION BASED ANONYMOUS ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

E.Devipriya[1], Dr.P.Ganesh kumar[2]

[1]Department of Information Technology, PSNACET, Dindigul

[2]Department of Information Technology, PSNACET, Dindigul

Abstract— Efficient defense against security attacks is a challenging task in the wireless sensor network and offering security guarantees becomes an important requirement in the design of the relevant networking protocols. In the existing system, anonymity is not completely offered to data sources, destination and routes where information's are exposed to malicious nodes. The situation is further aggravated as the next generation wireless sensor network will be larger and larger. To face this problem, we propose a Location Based Anonymous Routing Protocol (LBARP) which adopts the geographical routing principle to cope with the network dimensions and relies on a distributed trust model (hidden servers) for the avoidance of malicious nodes. Once trust information is available for all network nodes, the routing decisions can take it into account, i.e. routing can be based on both location and trust attributes (hidden servers). In wireless sensor network the LBARP separates the location of source and destination by grids. The LBARP provides anonymity to source, destination and route to enhance security in wireless sensor networks. This paper can be implemented with LBARP in wireless sensor networks to achieve high anonymity.

Keywords*-LBARP, Anonymity, Hidden servers*

I INTRODUCTION

A Wireless Sensor Network is a self-configuring network of small sensor nodes which communicates among them deployed to sense, monitor and gather information about the physical world. WSNs are gaining attention as they have great potential for both research and commercial applications. The sensor network nodes themselves are ideally less expensive, tiny devices. Recent advances in wireless sensor networks of Wireless Sensor Networks (WSNs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. WSNs have attracted much attention due to its great potential to be used in various applications. The key requirement from both the technological and commercial point of view is to provide adequate security capabilities for the sensor nodes where WSNs are expected to be solutions to many applications, such as detecting and tracking the passage of troops and tanks on a battlefield, personnel in a building. Generally, adversaries are assumed to be able to undetectably take control of a sensor node and extract all secret data in the node. Fulfilling privacy and security requirements for WSNs is necessary to prevent the attacks from adversaries.

Sensor networks interact closely with their physical environments which may lead to many security problems. Consequently, existing security mechanisms are inadequate, and new ideas are needed. Like **traditional networks, most sensor network applications** require protection against **eavesdropping, injection, and modification of packets.** Cryptography is the standard defense that can provide complete security to the sensor nodes. Interesting system trade-offs arise when incorporating cryptography into sensor networks. **For point-to-point communication, end-to-end cryptography achieves a high** level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast.Security can be enhanced from outside attackers by providing anonymity to the sensor nodes[7][6]. Anonymous routing protocols are crucial for WSNs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in WSNs includes identity and location anonymity of data sources (i.e., senders) and base station (i.e., recipient), as well as route anonymity. It is hard if possible for other nodes to obtain the real identities and exact locations of the sources and base station. For route anonymity, adversaries cannot trace a packet flow back to its source or destination by tracing their route and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to segregate the connection between source and destination (i.e., relationship unobservability), it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in WSNs where location devices may be equipped.

II RELATED WORKS

AO2P: AD HOC ON-DEMAND POSITION-BASED PRIVATE ROUTING PROTOCOL- Anonymity for a destination relies on the difficulty of matching a geographic position to a real node ID. This can be enforced by the use of secure position service systems. Node mobility enhances

ISSN 2348 - 7968

destination anonymity by making the match of a node ID with a position momentary. To further improve destination privacy, R-AO2P is proposed. In this protocol, the position of a reference point, instead of the position of the destination, is used for route discovery. Analytical models are developed for evaluating the delay in route discovery and the probability of route discovery failure. A simulator based on ns-2 is developed for evaluating network throughput. Analysis and simulation results show that, while AO2P preserves communication privacy in ad hoc networks, its routing performance is comparable with other position-based routing algorithms. The disadvantages of AO2P are a node does not hide their ID in the network for building a route, sending or receiving data, are highly traceable and, consequently, nodes are vulnerable to attacks and disruptions, the bandwidth is limited, it is not easy to maintain such a group with a fixed proxy in an ad hoc network due to the node mobility and the continuous join-and-leave activities, the cost of using public keys is high.

ALARM: Anonymous Location-Aided Routing in Suspicious MANETs - Some interesting issues arising in MANETs by designing an anonymous routing framework (ALARM). It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and intractability (tracking-resistance). It also offers resistance to certain insider attacks. MANET environment, it is natural to require that node movements be obscured, such that tracking a given node (even without knowing its identity) is impossible or, at least, very difficult, suspicious and hostile MANET environments are (or will be) common, they do occur in military and law enforcement domains.

A Scalable Location Service For Geographic Ad Hoc Routing - GLS combined with geographic forwarding allows the construction of ad hoc mobile networks that scale to a larger number of nodes[3]. GLS is decentralized and runs on the mobile nodes themselves, requiring no fixed infrastructure. Each mobile node periodically updates a small set of other nodes (its location servers) with its current location. A node sends its position updates to its location servers without knowing their actual identities, assisted by a predefined ordering of node identifiers and a predefined geographic hierarchy.

In these networks require a large up-front investment in fixed infrastructure before they are useful—central offices, trunks, and local loops in the case of the telephone system, radio towers for the cellular network. Upgrading these networks to meet increasing bandwidth requirements has proven expensive and slow. Finally these services may not provide adequate service, or may be too expensive.

III LBARP

The Location Based Efficient routing Protocol provides anonymity to protect the sensor nodes from adversaries. The anonymity is achieved for both location and identity. As the GPS devices are not expensive the nodes are deployed with it. The location of each node is known and the network area is considered as grids to partition the location of source and destination. The source and destination are fixed in separate grids and the data are forwarded. cryptographic techniques are used to enhance security.

A.. Node Deployment

We assume the entire networks area as grids. The nodes are deployed in the wide area network with a GPS device. Nodes identify its location by the GPS device attached with it. Information about the top left and bottom right of the grids are computed to maintain the location of the nodes in the network area. The location information's are not shared with any other nodes without authentication. As the nodes are need to be secured from the adversary nodes source, route and destination anonymity is provided. The sender node selects a node randomly in the nearest zone and forwards the information to it. All the nodes in the source node zone forwards the information to the temporary forwarder in the nearest zone. The temporary forwarder collects the information and then sends it to the next temporary forwarder in its nearest zone. Similarly, the data are forwarded through the temporary forwarder until it reaches destination zone. This temporary forwarder is called as Random Forwarder. LBARP uses the randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

In this paper, the zone having n nodes where D resides is called as the destination zone, denoted as ZD. n is used to control the degree of anonymity protection for the destination. Specifically, in the LBARP routing, each data source or forwarder executes the consecutive selection of temporary forwarder. It first checks whether itself and destination are in the same zone. If so, it divides the zone in to smaller size. The node repeats this process until itself and ZD are not in the same zone. It then randomly chooses a node positioned in the other zone to forward temporarily, and then GPSR routing algorithm to send the data to the node closest to RF. This node is defined as a random forwarder (RF). LBARP aims at achieving n-anonymity for destination node D, where n is a predefined integer. Thus, in the last step, the data are broadcasted to n nodes in ZD, providing n-anonymity to the destination.

B. Providing Anonymity in Sensor Network

Anonymity in sensor networks means hiding the identity of the node from the nodes other than the message sender and the base station participating in a communication. It includes sender anonymity, receiver anonymity, route between the sender and receiver. Thus, an adversary cannot determine the sender and receiver's identities through reading a message intercepted from the network or through reading messages forwarded by a sensor node it has compromised, and the

ISSN 2348 - 7968

adversary also cannot determine whether two communication segments (i.e., message transmissions between two neighboring nodes) belong to the same communication between a sensor and the base station. There are two forms of anonymity.

1) Identity anonymity

Each node in the network will have an identity in the network. The adversary node observes the node behavior and communication by using its identity. The identity anonymity hides the identity of the node from other nodes in order to provide secure communication. The identity of the node is visible only to authenticated nodes in its vicinity. The malicious node which tries to communicate with the sensor node is identified by the nodes as it is not authenticated. The sensor node verifies its neighbor node's key whenever it wants to communicate.

2) Location anonymity

The location of the source, destination nodes and the route used for communication can be traced by the third parties and eavesdrop the data. Location anonymity is hiding the location of the nodes from other nodes (i.e hiding the location of source, destination and the routes from third parties). Concealing the current position of an entity is termed as location anonymity. Location anonymity also includes the concealment of the motion pattern of the entity. The location of the source nodes are hidden as the nodes other than source will also send dummy data to the RF along with the source in the same time. The base station or the destination identifies the data and discards the dummy data. This mechanism helps to achieve source anonymity. The route of the data cannot be traced as the data are gathered only by the intermediate nodes called as RF and then it is forwarded to the destination. Choosing the RF randomly makes the route untraceable by the adversaries. The destination anonymity is provided by disseminating the data to all the nodes in the destination zone, thus providing n-anonymity, where the n is the number of nodes in the destination zone.

C. The Destination Zone Position

We use ZD rather than D is to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone. The nodes should be aware of destination zone, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in ZD. Let H denote the total number of grids in order to produce ZD. Using the number of nodes in ZD (i.e., n), and node density ρ , H is calculated by

$$H=\log_2((\rho.G)/n)$$

where G is the size of the entire network area.

Procedure

LBARP

H: Total number of partitions
ρ: Node density
G: Size of network area
n: nodes in final zone
begin
consider Area (0,0) and (x_G,y_G)
calculate $H=\log_2((\rho.G)/n)$
x=0
for x is not equal to H
divide as grid
name zone Ax
select Random Forwarder (RFx)
forward data to Random Forwarder
end for
if zone D has n nodes
Broadcast data from RF to all nodes
end

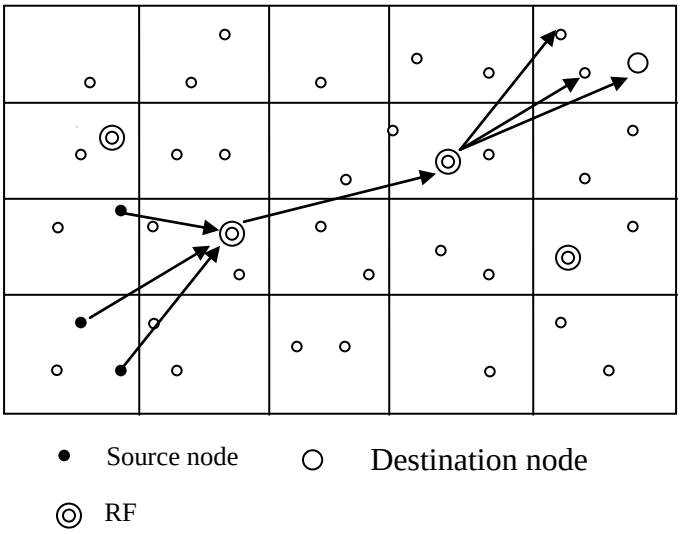


Fig 1 Nodes deployed in the wireless sensor network

In the fig.1, the sensor nodes send the sensed information are gathered by first random forwarder and the information are forwarded to the next Random Forwarder. This process repeats until it reaches the destination. In the destination zone the gathered information is broadcasted to all the nodes in order to provide destination anonymity.

IV SECURITY

The nature of wireless communications, resource limitation on sensor nodes, characteristics of the networks, unknown topology prior to deployment, and high risk of physical attacks to the sensor nodes, it is a difficult to provide security in WSNs. The ultimate security requirement is to

provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. Nodes must be secured from the attacks like jamming, tampering, spoofed routing information. To offer secure communications for the WSNs, security solutions depend on the use of strong and efficient key distribution mechanisms in uncontrolled environments. To implement a fundamental security service pair-wise key establishment should be used, enabling secure communications among the sensor nodes using cryptographic techniques. In the case where sensor nodes should use pre-distributed keys directly, or use keying materials to dynamically generate pair-wise keys, the main challenges is to find an efficient way of distributing keys and keying materials to sensor nodes prior to deployment.

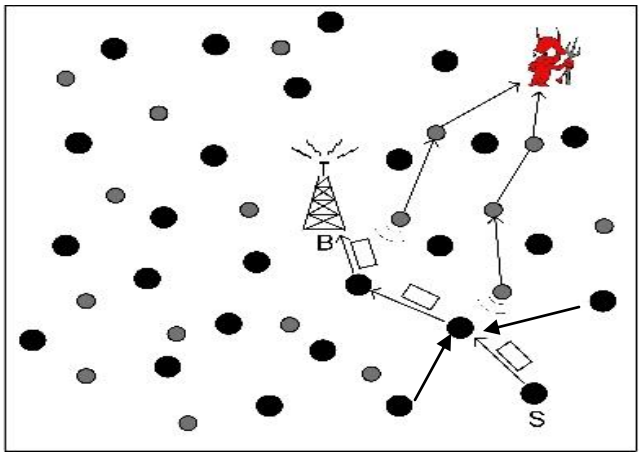


Fig 2. Malicious node in the network

The fig.2 describes the malicious node present in the wireless sensor network along with the sensor nodes. These adversaries try to observe the communication behavior using the identity of nodes and attack the routing nodes.

V. CRYPTOGRAPHIC TECHNIQUES

The routing of data is done using GPSR protocol by verifying its security key assigned during its deployment. The key distributor initializes the keys to nodes during its dissemination and whenever other mobile node joins the network the key is assigned to it. Malicious nodes cannot find the identity and location of the node as their identity and locations are anonymous[8].

A. Hidden Server / IKM (ID-based key management scheme)

In IKM, each node should carry an authentic ID-based public key pair at any time as a proof of its membership. With such key pairs, nodes can realize mutual authentication, key agreement, public-key encryption, and digital signatures, among other security services.

IKM consists of three phases:

- key pre-distribution
- Revocation
- Update.

1) Key pre-distribution

Key pre-distribution is a one-time process occurring during network initialization, where a Private Key Generator (PKG), essentially a trusted authority, generates a key based on node identity and preloads every node with appropriate keying materials.

In addition, the PKG distributes its functionality to 'n' number of D-PKGs selected among the N nodes to enable secure and robust key revocation and update during network operation.

2) Revocation

During network operation, when a node is suspected, say A, has been compromised, a node sends a signed accusation against A to D-PKGs. The accused A is diagnosed as compromised when the number of accusations against it reaches a predefine *revocation threshold*, in a certain time. At that point, the network enters the key revocation phase in which the D-PKGs jointly issue a key revocation against A.

3) Update

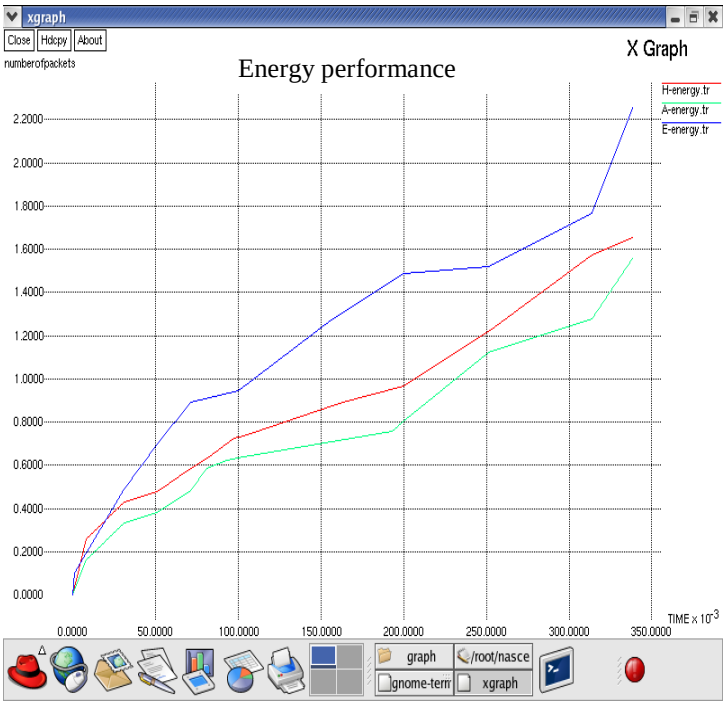
As a common practice, public keys of nodes need to be updated at intervals. The key update phase may occur either periodically according to a prescribed time period, or reactively when the number of revoked nodes attains some predetermined threshold. During this phase, each non-revoked node can update its public key autonomously and its private key via a single broadcast message. This is enabled by our novel public key construction method. Our scheme can also ensure that compromised nodes, once revoked, cannot get their keys updated, thus isolated from the network.

The PKG maintains a set of keys which allocates the key to the nodes based on their identity. The set of keys are assigned to each node in the network until all the generated keys are fixed. After assigning last key to the node, the PKG selects a key randomly from available keys to the remaining nodes .Once all the keys are assigned for node second time the keys may be used for third time for a node. The mobile node which enters the zone obtains a key from the PKG, which maintains a set of key. When the node moves out of the network area its key is revoked.

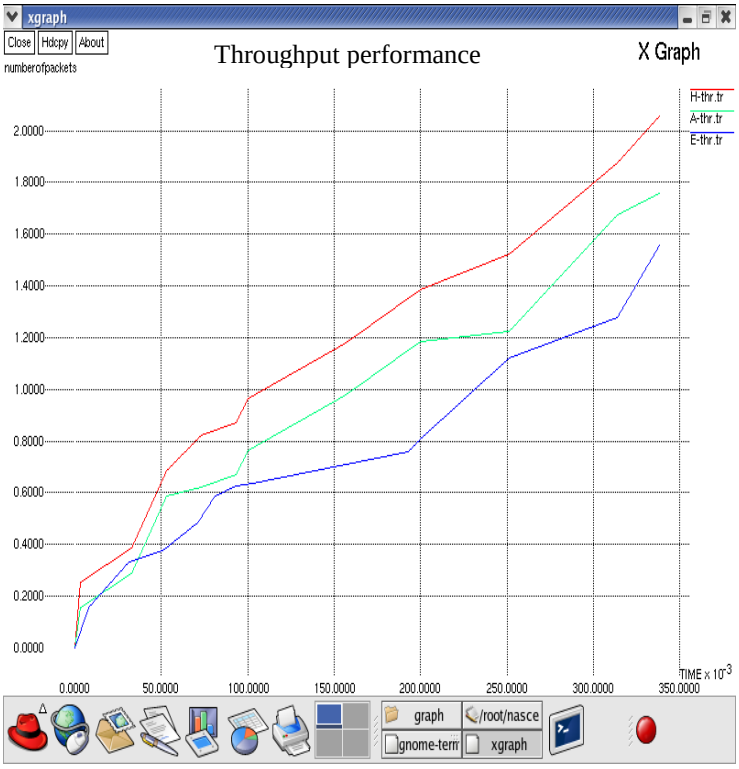
VI. PERFORMANCE EVALUATION

In this Section, we present the performance evaluation of LBARP (Location Based Anonymous Routing Protocol) using the NS2.

ISSN 2348 - 7968



Based on the simulation Analysis, the energy and throughput performance is high compared with other anonymity protocols. The Performance results shows LBARP shows better results. With the security implementations, all the Source nodes and base station are safe from malicious nodes.



IV CONCULSION

Some protocols are unable to provide complete source, destination, and route anonymity protection. LBARP is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic grid partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in LBARP includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. LBARP further strengthens the anonymity protection of source and destination by hiding the data initiator/destination among a number of data initiators/ destinations. It has the mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, LBARP has an efficient solution to attacks using the cryptographic techniques. LBARP ability to fight against timing attacks is also analyzed. Experiment results show that LBARP can offer high anonymity protection at a low cost when compared to other anonymity algorithms.

REFERENCES

[1] X. Wu, J. Liu, X. Hong, and E. Bertino, “Anonymous Geo- Forwarding in MANETs through Location Cloaking,” IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.
2] X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.
[3] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, “A Scalable Location Service for Geographic Ad Hoc Routing,” Proc. ACM MobiCom, 2000.
[4] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
[5] K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.
[6] Slava Kisilevich, Lior Rokach, Yuval Elovici, and Bracha Shapira, “Efficient Multidimensional Suppression for K-Anonymity”,IEEE Transactions on Knowledge and Data Engineering, , March 2010.
[7] Bu_gra Gedik and Ling Liu, ”Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms”, IEEE Transactions On Mobile Computing, January 2008.
[8] jiyanbo yao,”A Security Architecture for Wireless Sensor Networks Based-On Public Key Cryptography”, International Conference on Wireless communication, Networking and Mobile computing,2009