Location Privacy Preservation of Sink through Multi-Path Selection in WSN

[1]Deepika H.T, [2]Chinnaswamy C.N, [3]T.H Srinivas.

[1]PG Student, [2]Associate Professor, [3]Professor
[1,2]Department of ISE,
[3]Department of Computer Science
[1,2]The National Institute of Engineering, Mysuru, India
[3]VVCE, Mysuru

***Abstract*-Wireless Sensor Networks (WSN) is one of the main zone of research and it has been more well known in the real life difficulties by giving minimal effort arrangements. The system comprises of little sensor nodes capable for detecting, handling, computation and communication. The system comprises of various sorts of assault, the most harming assault is sinkhole assault. In this kind of assault, the sinkhole node tries to draw in information to itself by transmitting counterfeit data to neighbor nodes and henceforth it interferes with the usefulness of such systems. Thusly with a specific end goal to overcome from this sort of assault giving security is critical. In this paper we are proposing sink and also source area protection systems. With a specific end goal to give more protection these procedures like forward random walk (FRW) and BLAST (Base station location anonymity and security technique) is utilized. On account of forward random walk conspire requires every node to acquire its hop count to the sink, which can be accomplished by utilizing a sink-based flooding. Toward the starting, the sink will start a flooding, after which every node can get the both its neighbors hop count to the sink. On account of BLAST conspire the center thought is to change the transmission scope of an arrangement of some chose sensors around the base to befuddle the assailant. Through this procedure, we can make an arrangement of fake base stations which can't be recognized by a solid assailant. Simulation results demonstrate these two techniques, Simulation is carried out using simulator NS3.**

Keywords-Wireless Sensor Networks (WSN), Base station Location Anonymity and Security Technique (BLAST), Forward Random Walk (FRW), Location Protection Routing(LPR), Two phantom nodes.

I. INTRODUCTION

Wireless Sensor network arrange comprises of minute sensor nodes, low-power, light weight, minimal effort. Because of the ease of these nodes, the situating can be in the request of result of thousands to million nodes. The sensor nodes perform desire estimations, process the information and send it to a base station, which is usually referred to as sink node. The base station gathers the information from every one of the nodes and assesses the information from every node Base station assumes an imperative part in WSN. Aside from sensor nodes the base station it contains an extensive number of computational power, it has bigger memory. Be that as it may, sensors utilizes bring down power, bring down transmission capacity. Consequently the numerous sensors convey to the closest base station. The WSN comprises of numerous number of nodes every node is associated with at least one sensors. Every node comprises of a few sections like radio handset alongside a reception apparatus, and a microcontroller, is an electronic circuit, which associates sensors and a vitality source i.e., battery. Contingent on the size and asset restriction in sensor nodes, for example, memory, data transfer capacity, computational speed a sensor node may differ in estimate.

Keeping in mind the end goal to spare computational vitality in WSN, it is important to lessen a portion of the messages that is transmitted to the aggregation points. This can be dodged by utilizing some aggregation algorithm i.e., brute force algorithm it is conceivable to postpone messages to a specific degree. There are numerous application in sensor arrange. This incorporates military application is utilized to control the following, identifying and observation of the outskirts. Aside from this different applications incorporate ecological applications, home applications, and business applications.

Sinkhole assault is an insider assault, where an aggressor dispatches this sort of assault by trade off a node inside the system. At that point that node with the assistance of neighbor node which will tries to attract all the traffic by utilizing some routing protocol. By accomplishing this, the assailant dispatches an assault. Here the communication takes place in the form of many to one for this situation, where every node send data to base station, make this WSN unprotected from sinkhole assault.

Sinkhole assault ordinarily works like this as shown in **Fig. 1**[1], it tries to draw in neighbor nodes, it tries to pull in neighbor nodes by making damaging node which looks precisely like the original node with the assistance of routing algorithm. By making this, when a foe forward a few information packets the neighboring node of the enemy that it is a decent quality. Thus it is going ahead every one of its neighbors. So every one of the information are gathered by ruinous node which is under the control of enemy. He has the ability to change or even may drop the information packet and may harm the whole system.

Base station is a sort of radio transmitter or recipient it contains of low-control transmitter and wireless router it acts as a node of the local wireless network and may likewise it goes about as a gateway between a wireless and wired system. The primary motivation to kept base station in sinkhole assault is it detects the information accurately from the key hazard. Typically, this occurs in open regions, because of some powerless wireless associations.

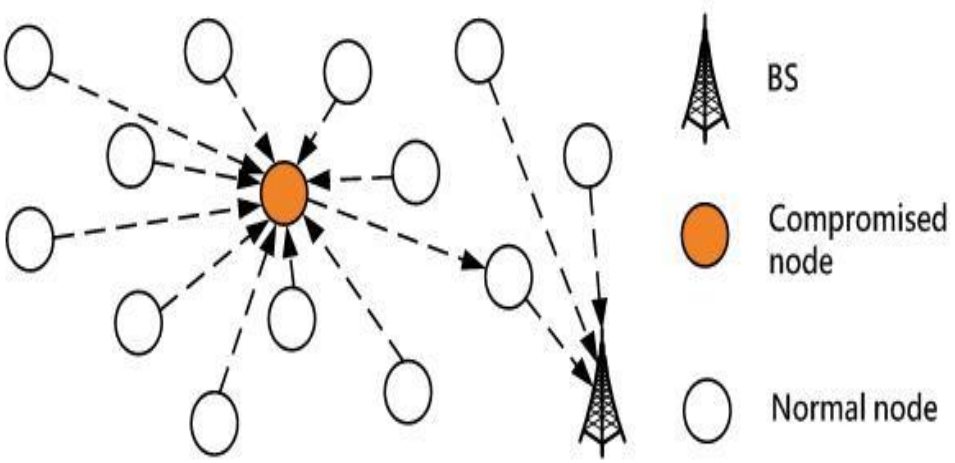

Figure 1: Sink Hole Attack

Safeguarding of sink is all the more difficult task in sensor network, because of the absence of accessibility of vitality, communication and computation assets which prompt light weight, vitality productive and security safeguarding components. For instance: If the sensors utilize the minimal effort radio gadget transmitters or receivers and some institutionalized wireless communication advances then it is simple for a intruder to trap the correspondence amongst sensor and catch the significant data.

Henceforth it is critical to deal with protection and furthermore vitality utilization. And furthermore it is critical to keep delay as least as could reasonably be expected. By accomplishing this, the information may even now valuable in the event that it ranges to the base station. .

Types of attacks and security threats in Wireless Sensor Networks:

Table 1: Layer wise attacks in WSN

Attacks	Layer affected	Security threats
Jamming, Tampering	Physical	Availability, Integrity
Collisions, Exhaustion, Unfairness	Data Link layer	Confidentiality, Integrity
Spoofing, Selective Forwarding, Sybil, sinkhole, Wormhole, Node Replication	Network Layer	Availability, Authentication, Confidentiality
Availability, Authentication, Confidentiality	Transport Layer	Availability

II. RELATED WORK

Providing location privacy in sensor network is major challenging errands. By utilizing a few procedures if interloper decides the source and destination at that point there might be a shot that assailant can devastate the entire system. In location privacy there are two noteworthy undertakings which may encourages for the interloper to find their objectives, in particular by recognizing the movement of nodes and by the traffic pattern. There are a few ways that an interloper can follow the location one is packet headers which contain the whole data of source and destination, consequently ensuring this sort of data is critical in accomplishing location privacy. Consequently a few creators underlined a few techniques to ensure the privacy protection against nearby spy.

III. LOCATION PRIVACY TECHNIQUES

In this scheme [2] sink anonymity is one of the fundamental issues regarding giving security. By utilizing encryption and authentication it isn't conceivable to safeguard sink location. Since through traffic analysis one can without much of a stretch distinguish its location. To stay away from every one of these issues CSL (concealing of the sink location) strategy is utilized, for the most part it comprises of utilizing fake message injection. CSL completed a successful work as far as securing sink's location. It shields important data from the aggressors. In spite of the fact that, it works viable in protecting the significant information from the interloper however it makes more traffic in the system by sending fake messages and furthermore fake messages consumes heaps of vitality which additionally prompts poor performance as far as throughput and delay.

In this scheme [3] the system LPR (location protection routing) protocol is utilized, for the most part to keep away from for an interloper to barge in or catch the beneficiary's location. Joining with fake packet injection, LPR tries to stay away from traffic so

the data may not be accessible for an assailant to listen in. The LPR strategy going to confuse the direction of incoming and outgoing traffic and it is distributed consistently. With the goal that an enemy hard to distinguish the data in the network. Despite the fact that it gives more security to the beneficiary location yet it faces an issue in communication and computation overhead.

The other routing protocol which is called as phantom routing protocol is utilized to secure the location privacy of source nodes. In each phantom routing before coming to the sink every single packet takes an irregular walk. This happens chiefly to befuddle an aggressor with the goal that an assailant may neglect to venture into the right goal. Once in a while there might be a possibility that interloper can distinguish the source node location. This can be stayed away from by utilizing two phantom nodes in the network. Two phantom nodes can be chosen such that no two phantom nodes which are of same triplet are co-linear with sink. Two phantom nodes have ability to produce distinctive way for various packets for a similar network. Thus there might be a confusion emerges for an aggressor to discover the source location. This outcomes in limiting hit-ratio by maximizing the security.

In this scheme [4] to recognize sinkhole assault message digest algorithm is utilized, compromised node is essential on account of sinkhole assault in light of the fact that compromised node attracts other neighboring or encompassing nodes by utilizing some routing algorithm. For this situation the interloper sends malevolent node to interrupt a portion of the data in base station. At the end of the day, a gatecrasher may make a destructive node as compromised node with the goal that other node may neglect to recognize that node is a malignant. Henceforth it is important to ensure the original compromised node and furthermore messages which is sent between source to destination by utilizing forward routing path it is conceivable to distinguish sinkhole assault. To give greater security message digest algorithm is utilized, it basically comprises of one-way hash alongside cryptographic primitives. This outcomes in limiting computation overhead by boosting communication overhead.

In the rest of this paper, we will discuss the various techniques for location privacy of sink in WSN.

IV. TECHNIQUES TO HIDE THE LOCATION OF SINK

- Forward random walk

In this scheme [5] each node transfers a received packet to a node haphazardly chosen from its forward neighbors whose hop-count to the sink is no bigger than its own. This procedure is rehashed at every node until the point that the packet comes at the sink. Consider a sample network, in the source sends packet periodically to the sink by multi-hop wireless communication Tr. In the event that the packets dependably venture out from the source to the sink along a fixed path, it will be simple for a foe to catch either the source or the sink through hop-by-hop tracing. The FRW [5] requires every one of the nodes acquire their hop count to the sink, which can be accomplished utilizing a sink-based flooding.

Toward the finish of the flooding, every node can get both of its own particular and its neighbors hop count to the sink. In the FRW scheme, each node isolates its neighbor into three lists, further list, equivalent list and closer list. Each neighbor in the further list contains bigger hop count than the sender, though neighbor in the closer list has a smaller hop count than itself. Furthermore, the node in the equivalent list contains a smaller hop count with itself. The combination of the equivalent list and closer list forms the forward list.

Figure 2 indicates one of the message conveyance ways of the FRW scheme. When sending a packet, the node will arbitrarily choose a neighbor from its forward list as the next hop. Neighbors in the further list won't be considered as the contender for the next hop since they will naturally expand the latency.

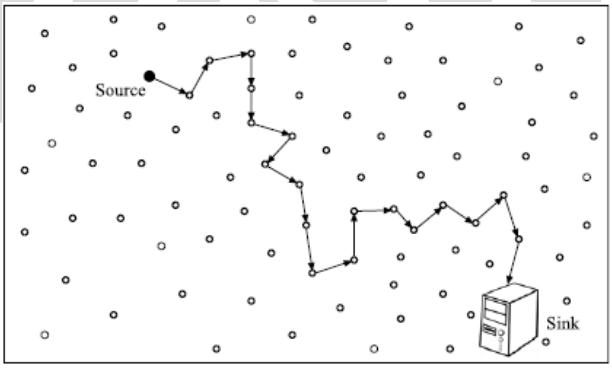

Figure 2: The scenario for the forward random walk scheme.

- BLAST (Base Location Anonymity and Security Technique)

BLAST [6] expects to secure the base station from both packet tracing and traffic analysis assaults and give great protection against the global assailant. Network is separated into blast nodes and ordinary nodes. Collector is available some place nearby blast nodes. Source node sends packet to one of the blast nodes which is then retransmitted inside blast area. The enemy is uninformed of the communication between blast node and real beneficiary. Henceforth location privacy of the collector is kept up.

An example of blast routing can be seen in

Figure 3. The source A arbitrarily picks a blast node B from the ring. At that point, the packet is routed from A to B through the most limited path between them. The node B now blasts the packet with a transmission scope of K × tx which is the width of the

security rings. This covers the entire ring and furthermore some additional nodes outside the ring. The real base station can be found anywhere inside the ring. To the foe, any node in the ring could be the base station. The significant preferred standpoint of this blast nodes strategy over the system depicted above is the energy consumption. Blast nodes procedure expends significantly less energy as just a single node in the path needs to transmit with more vitality for each packet and whatever remains of the path devours minimum conceivable energy.

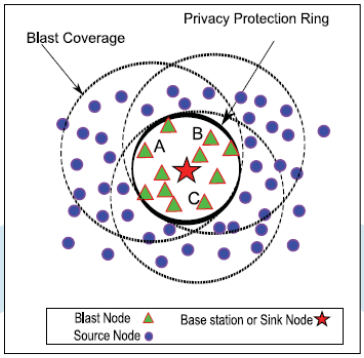

Figure 3: Working of blast node

V. EXPERIMENTAL RESULTS

In this section, we plan implementation framework of proposed algorithm using latest version 3.23 of NS3.

- Blast technique

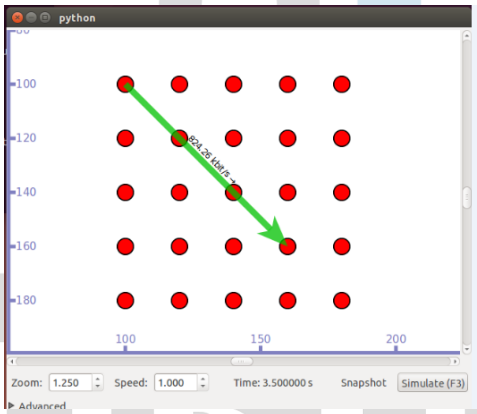

Figure 4: Source sending packet to destination

In this case source start sending packets to the destination as shown in the above **Fig. 4** starting node is taken it as Source node, 19th node is taken it as destination or sink node and remaining all other nodes are WSN nodes. While forwarding the packet the node will randomly selects its neighbor as next hop.

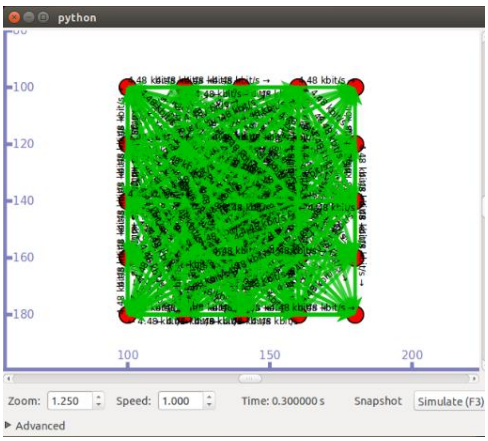

Figure 5: All nodes sending packet to destination

In this case source and all other nodes are start sending packets to the destination if anything happen while transmitting data to the destination or if intruder identify the path from where packet is coming and reaches into the destination then source node will

immediately update its routing information It is difficult for an attacker to find out the path, because all nodes are continuously sending its packets to the destination.

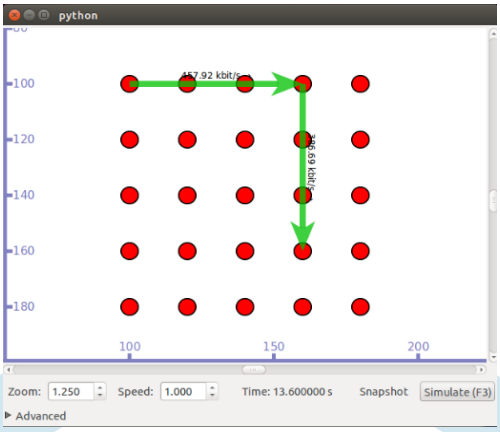

Figure 6: Source node changed its data transmission path

In this case the source node contains all routing information if an intruder identifies the path from where the packet is sending and from which node the packet is delivering into the destination, then source node will immediately updates its routing information and changes its link and it finds out which is nearest path to send packets to the destination which is shown in the above **Fig 6**.

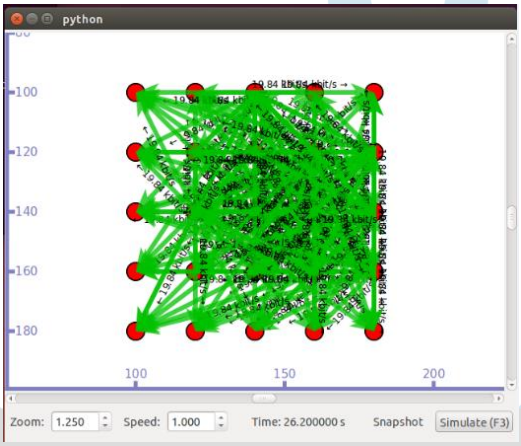

Figure 7: Source and other nodes changes its path

In this case after source node update its new routing information all other nodes also start transmits its data with the help of new path to reach into its destination. This procedure repeats until destination gets complete information which is shown in the above **Fig. 7**.

- **Forward Random Walk Technique**

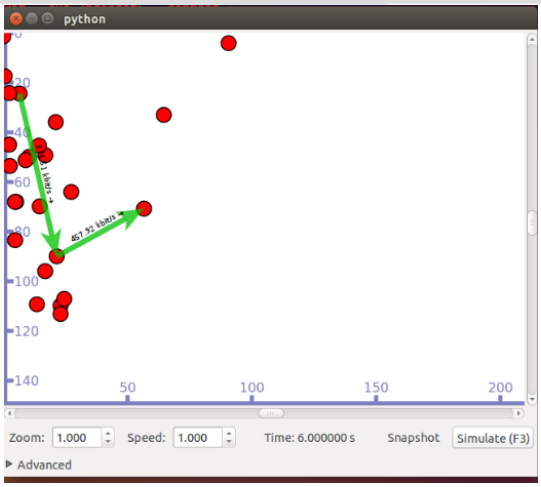

Figure 8: Randomly selected source and destination path

In this case we selected source node and destination node randomly, we can increase the transmission range using blast, source node which contains all the routing information for each transmission source node updates its routing information, QoS can be

achieved by keeping delay as less as possible.

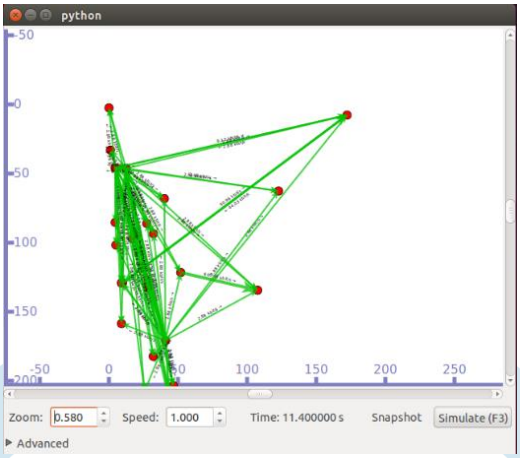

Figure 9: All nodes transmitting data to the randomly selected destination

In this case once source node start sending the data to the destination and all other nodes also start sending its data to the destination for each transmission routing information is updated in the source node.

VI. COMPARISON OF ALL TWO TECHNIQUES

- Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of successfully received packets by the destination to the total number of packets sent by the sender or source. Mathematically it can be defined as: PDR=S1/S2, where S1 indicates the sum of data packets received by the destination and S2 indicates sum of data packets sent by the sender. Graph show the data packets that are successfully delivered during simulation ratio of data packets versus number of nodes.

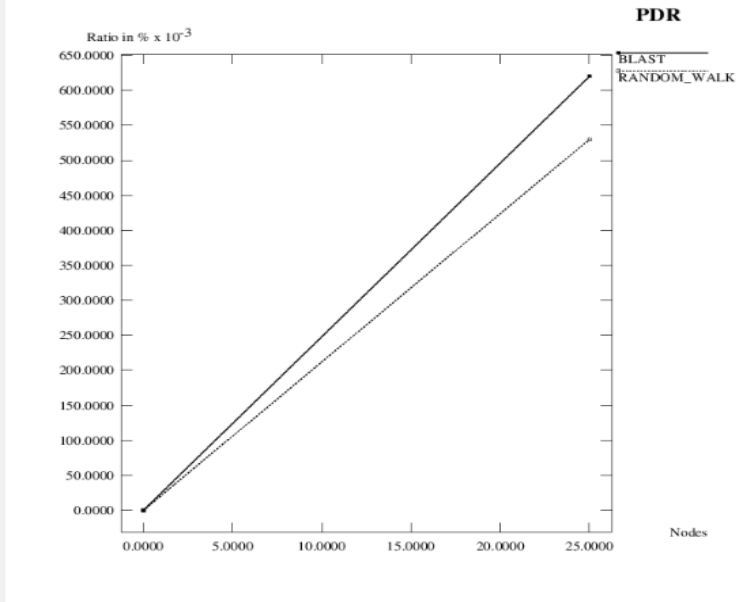

Figure 10: Packet delivery ratio in all two techniques

As shown in **Fig. 10**, the blast has more packet delivery ratio (PDR) when compared to forward random walk.

- Throughput

Throughput can be defined as it is the amount of rate at which information or data is sent through the network. Throughput is usually expressed in terms of bps. Graph show the data packets that are successfully delivered during simulation time versus number of nodes.

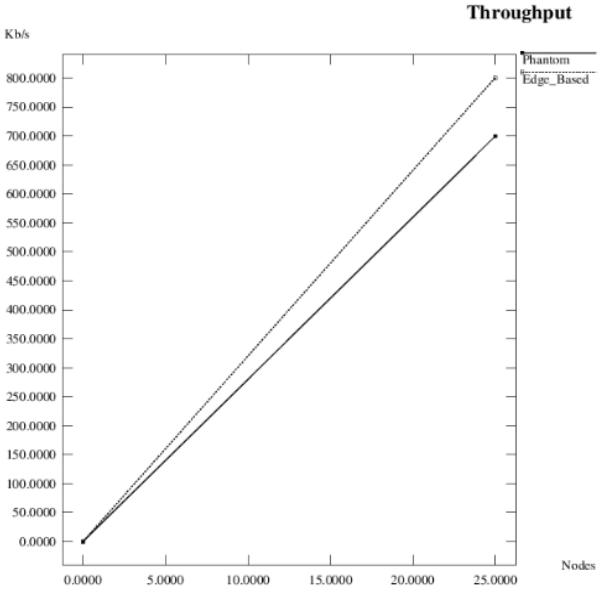

Figure 11: Throughput in all two techniques

As shown in **Fig. 11**, the blast has more throughput when compared to forward random walk.

VII. CONCLUSION AND FUTURE ENHANCEMENT

In our approach, we hide the location of sink from intruder using Blast and Forward Random Walk. Throughput is more in Blast when compared to Forward random walk Technique. Our work also motivates further research on Energy Consumption in Forward Random Walk and Blast Techniques. They can also research on proposing new techniques based on our ideas. The proposed protocol may be further enhanced by including other privacy preservation techniques.

REFERENCES

[1] S. Ahmad Salehi; M. A. Razzaque; Parisa Naraei; Ali Farrokhtala; "Detection of sinkhole attack in wireless sensor networks",2013 IEEE International Conference on Space Science and Communication (IconSpace),pp.361-365.

[2] Bidi Ying; Jose R. Gallardo; Dimitrios Makrakis; Hussein T. Mouftah; "Concealing of the Sink Location in WSNs by artificially homogenizing traffic intensity" 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),pp.988-993.

[3] Ying Jian, Liang Zhang, and Shigang Chen, "Protecting Receiver Location Privacy in Wireless Sensor Networks," IEEE INFOCOM 2007 proceedings. pp. 1955-1963.

[4] S. Sharmila and G. Umamaheshwari, "Detection of Sinkhole Attack in WSN using message digest algorithm," 2011 International conference on IEEE.

[5] H. chen and W. Lou, "From nowhere to somewhere: protecting end-to-end location privacy in WSN," 2010 International conference on IEEE.

[6] Venkata Praneeth Varma Gottumukkala; Vaibhav Pandit; Hailong Li; Dharma P. Agrawal,"Base-station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks", 2012 IEEE International Conference on Communications (ICC),pp.6705 – 6709.