Global Journal of Computer Science and Technology
Volume 11 Issue 18 Version 1.0 October 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Improved Privacy in Wireless Sensor Network Using QOS Routing Protocols

By Tenali. Nagamani, Damineni.SreeLakshmi

Dept of CSE PVPSIT Kanuru, Vijayawada

Abstract - Full network level privacy has often been categorized into four sub-categories:Identity, Route, Location and Data privacy. Achieving full network level privacy is a challenging problem due to the conditions imposed by the sensor nodes (e.g., energy, memory and computation power), sensor networks (e.g., mobility and topology) and QoS issues (e.g., packet reach-ability and timeliness). This proposed paper consists of two algorithms IRL algorithm and data privacy mechanism that addresses this problem. The proposed system provides additional trustworthiness, less computation power, less storage space and more reliability. Also, we proved that our proposed solutions provide protection against various privacy disclosure attacks, such as eavesdropping and hop-by-hop trace back attacks.

Keywords : *anonymity; eavesdropping; hop-by-hop trace back; privacy; routing; wireless sensor networks.*

GJCST-F Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Improved Privacy in Wireless Sensor Network Using QOS Routing Protocols

Tenali. Nagamani [α], Damineni.SreeLakshmi [Ω]

Abstract - Full network level privacy has often been categorized into four sub-categories: *Identity*, *Route*, *Location* and *Data* privacy. Achieving full network level privacy is a challenging problem due to the conditions imposed by the sensor nodes (e.g., energy, memory and computation power), sensor networks (e.g., mobility and topology) and QoS issues (e.g., packet reach-ability and timeliness). This proposed paper consists of two algorithms IRL algorithm and data privacy mechanism that addresses this problem. The proposed system provides additional trustworthiness, less computation power, less storage space and more reliability. Also, we proved that our proposed solutions provide protection against various privacy disclosure attacks, such as eavesdropping and hop-by-hop trace back attacks.

Keywords : anonymity; eavesdropping; hop-by-hop trace back; privacy; routing; wireless sensor networks.

I. Introduction

In order to present the adversary from back-tracing, the route, location and data privacy mechanism must be enforced. With the spreading application of Wireless Sensor Networks (WSNs) in various sensitive areas such as health-care, military, habitat monitoring, etc. Network level privacy often been categorized into 4 categories:

1. Sender node identity privacy: no intermediate node can get any information about who is sending the packets except the source, its immediate neighbors and the destination.
2. Sender node location privacy: no intermediate node can have any information about the location (in terms of physical distance or number of hops) about the sender node except the source, its immediate neighbors and the destination.
3. Route privacy: no node can predict the information about the complete path (from source to destination). Also, a mobile adversary gets no clue to trace back the source node either from the contents and/or directional information of the captured packet(s).
4. Data packet privacy: no node can see the information inside in a payload of the data packet except the source and the destination.

Author [α] : M.Tech, CSE, PVPSIT, Kanuru, Vijayawada.
E-mail : tenalinagamani@gmail.com
Author [Ω] : M.Tech, Vijayawada, Asst. Professor, Dept of CSE PVPSIT, Kanuru, Vijayawada. E-mail : damineni.mtech@gmail.com

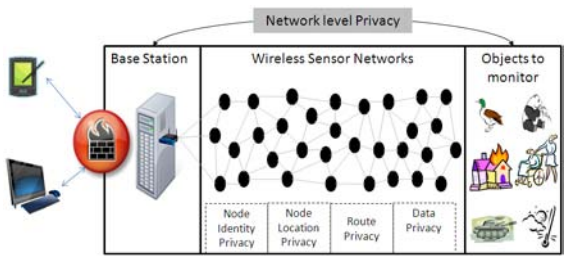
An energy-efficient privacy solution is needed to address these patterns in Wireless Sensor Network. Advanced features in cryptographic system were introduced in this paper are:

- A new Identity, Route and Location (IRL) privacy algorithm is proposed that ensures the source, identity and location. This algorithm allows the packets to destination only through trusted intermediate nodes.
- The extension of our proposed IRL algorithm is a new reliable Identity, Route and Location (r-IRL) privacy algorithm. This algorithm has the ability to forward packets from multiple secure paths to increase the packet reach-ability.
- A data privacy mechanism is used to unique in the sense that it provides secure data and packet authentication.

a) Network and Assumptions Model

A wireless sensor network (WSN) is composed of large number of small sensor nodes that are of limited resource and densely deployed in an environment. This sensor node uses IEEE 802.11 standard link layer protocol, which keeps packets in its cache until the sender receives an acknowledgment (ACK). The sender node will retransmit the packet, if the ACK does not receive within threshold.

Figure 1 : Typical WSN scenario.



II. Proposed Scheme

a) Concepts and Definitions

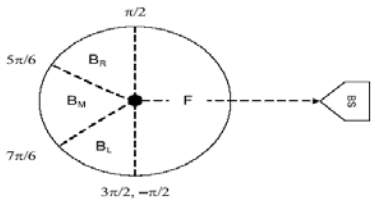
The proposed algorithms use two notions: Direction and Trust. These notions are used to provide reliable secure paths for achieving robust route privacy. Direction helps to forward packet to the destination in a timely manner and trust will help to forward the packets via reliable nodes.

Direction: The first notion used in our algorithms is that of direction. The physical location of the base station is the reference point for each sensor node. Based on this reference point, each node classifies its neighboring nodes into four categories: (1) forward neighboring nodes (F), (2) right side backward neighboring nodes (Br), (3) left side backward neighboring nodes (B_l), and (4) middle backward neighboring nodes (B_m). The objective of this categorization is to provide more path diversity as discussed in Section 4.2. A node x classifies its neighboring node y in following fashion :

$$C_{x,y} = \begin{cases} F & \frac{-\pi}{2} \leq \theta \leq \frac{\pi}{2} \\ B_r & \frac{\pi}{2} < \theta \leq \frac{5\pi}{6} \\ B_m & \frac{5\pi}{6} < \theta \leq \frac{7\pi}{6} \\ B_l & \frac{7\pi}{6} < \theta < \frac{3\pi}{2} \end{cases}$$

Where θ is the angle between the node x and its neighboring node y with respect to the line joining node x and the base station as shown in Figure 2.

Figure 2 : Neighbor node classification



Trust: The second notion used in our algorithms is that of trust. The definition of a trust here is based on our other paper and restated here. A node can be classified into one of the three categories: trustworthy, untrustworthy, and uncertain. A node is considered trustworthy if it interacts successfully most of the time with the other nodes. A node is considered untrustworthy if it tries to do as many unsuccessful interactions as possible with the other nodes. An untrustworthy node could be a faulty or malicious node. A node is considered uncertain if it performs both successful and unsuccessful interactions. Detailed definition if the successful and unsuccessful interactions and trust calculation methodology is available in our paper and provided here in a simplified form.

A sender will consider an interaction successful if the sender receives confirmation that the packet is successfully received by the neighbor node and forwarded towards the destination in an unaltered fashion. The first requirement of successful reception is achieved on the reception of the link layer acknowledgment (ACK). The second requirement of forwarding towards the destination is achieved with the help of enhanced passive acknowledgment (PACK) by overhearing the transmission of a next hop on the route, since they are within the radio range. If the sender node does not overhear the retransmission of the packet within a threshold time from its neighboring node or if the overheard packet is found to be illegally fabricated (by comparing the payload that is attached to the packet), then the sender node will consider that interaction as unsuccessful.

With this simple approach, several attacks can be prevented, i.e., the black hole attack is straightforwardly detected when malicious node drops the incoming packets and keeps sending self-generated packets .Similarly, sink hole attack, an advanced version of the black hole attack, is also easily detectable by looking at the passive acknowledgment. Likewise, the selective forwarding attack and gray-hole attack [27] can also be eliminated with the aid of above mentioned approach. Based on these successful and unsuccessful interactions node x can calculate the trust value of node y in following fashion:

$$T_{x,y} = \left[100\left(\frac{S_{x,y}}{S_{x,y}+U_{x,y}}\right)\left(1-\frac{1}{S_{x,y}+1}\right)\right]$$

Where [.] is the nearest integer function, $S_{x,y}$ is the total number of successful interactions of node x with y during time δt, and $U_{x,y}$ is the total number of unsuccessful interactions of node x with y during time δt. After calculating trust value, a node will quantize trust into three states as follows:

$$Mp(T_{x,y}) = \left\{ \begin{array}{cc} \text{trustworthy} & 100 - f \leq T_{x,y} \leq 100 \\ \text{uncertain} & 50 - g \leq T_{x,y} < 100 - f \\ \text{untrustworthy} & 0 \leq T_{x,y} < 50 - g \end{array} \right\}$$

Where, f represents half of the average values of all trustworthy nodes and g represents one-third of he average values of all untrustworthy nodes. Both f and g are calculated as follows:

$$f_{j+1} = \begin{cases} \left[\frac{1}{2}\left(\frac{\sum_{i \in R_x} T_{x,i}}{|R_x|}\right)\right] & 0 < |R_x| \leq n-1 \\ f_j & |R_x| = 0 \end{cases}$$

$$g_{j+1} = \begin{cases} \left[\frac{1}{3}\left(\frac{\sum_{i \in M_x} T_{x,i}}{|M_x|}\right)\right] & 0 < |M_x| \leq n-1 \\ g_j & |M_x| = 0 \end{cases}$$

The steady-state operation, these values can change with every passing unit of time which creates dynamic trust boundaries. After each passage of time, Δt, nodes will recalculate the values of f and g. This trust calculation procedure will continue in this fashion.

The time window length (Δt) could be made shorter or longer based on the network analysis scenarios. If Δt is too short, then the calculated trust value may not reflect the reliable behavior. On the other hand, if it is too long, then it will consume too much memory to store the interaction record at the sensor node. Therefore, various parameters can be used to adjust the length of Δt.

Where [.] is the nearest integer function, Rx represents the set of trustworthy nodes for node x, Mx the set of untrustworthy nodes for node x, and n is the total number of nodes that contains trustworthy, untrustworthy and uncertain nodes. The initial trust

values of all nodes are 50.The values of f and g are adaptive.

b) Identity, Route, and Location Privacy (IRL)

The proposed identity, route and location privacy scheme works in two phases. The first is neighbor node state initialization phase, and the second is routing phase.

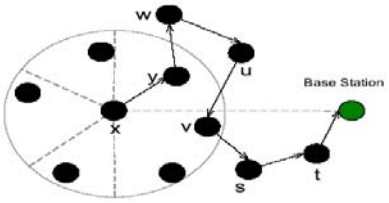
Route Privacy: In initialization phase, let the node i have m neighboring nodes in which t nodes are trusted. So, $0 \leq t \leq m$ and $M(t) = M(tF) \cup M(tBr) \cup M(tBl) \cup M(tBm)$. Here $M(tF)$, $M(tBr)$, $M(tBl)$, and $M(tBm)$ represent the set of trusted nodes that are in the forward, right backward, left backward, and middle backward directions, respectively. These neighbor sets ($M(tF)$, $M(tBr)$, $M(tBl)$,and $M(tBm)$) are initialized and updated whenever a change occur in neighborhood. For example, the entrance of a new node, change of a trust value, *etc*.

Whenever a node needs to forward a packet, the routing phase for source node and for intermediate node) of IRL algorithm is called.

Whenever a source node wants to forwards the packet, it will first check the availability of the trusted neighboring nodes in its forward direction set $M(tF)$. If trusted nodes exists then it will randomly select one node as a next hop from the set $M(tF)$ and forward the packet towards it .If there is no trusted node in its forward direction, then the source node will check the availability of a trusted node in the right ($M(tBr)$) and left ($M(tBl)$) backward sets. If the trusted nodes are available then the source node will randomly select one node as a next hop from these sets and forward the packet towards it.If the trusted node does not exist in these sets either, then the source node will randomly select one trusted node from the backward middle set ($M(tBm)$) and forward the packet towards it.If there are no trusted nodes available in all of the sets then the packet will be dropped .

When an intermediate node receives the packet (either from the source node or from another en-route node), it will first check whether the packet is new or old.If it is new, then the node will first check the availability of the trusted node from the forward direction set (*MF*) excluding the *prevhop* node if it belongs to forward set.If trusted nodes exists in the forward set then the node will randomly select any one trusted node as a next hop and forward the packet towards it. If there is no trusted node available in the forward direction, then it will check to which set the sender of the packet belongs to. For example, If the packet, forwarded by a node, belongs to the right backward set, then it will first check whether the left or middle backward sets contain any trusted nodes. If so, it will randomly select one node from those sets and forward the packet towards it. If there is no trusted node in those two sets, then the node will randomly select a trusted node from the right backward set ($M(tBr)$) excluding the one from which the node received the current packet and forward the packet towards it.Similar operations will be performed, if the packet, forwarded by a node, belongs to the left and middle backward or forward sets. An example IRL routing scenario is shown in Figure 3.

Figure 3 : Sample routing scenario of IRL scheme.

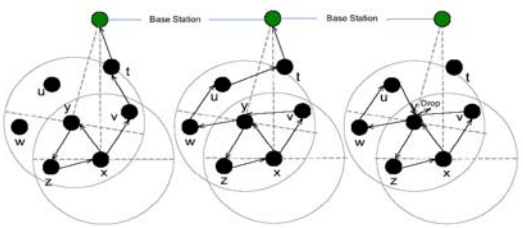


This routing strategy may result in the creation of a cycle (loop). However, due to the randomness in the selection of the next-hop and the presence of the different four direction sets, the probability of creation of any cycle is very low. Nevertheless, in order to fully avoid the occurrence of the cycles, each node (prior to forwarding of a packet) will save the signature of the packet in the buffer for the δt time,that is:

$$\delta t = 2\left(\frac{D}{d} \times p_t\right)$$

Where D is the distance between the forwarding node and the base station, d is the distance between the forwarding node and the next hop, and pt is the propagation transfer time between the forwarding node and the next hop. This signature consists of two fields: (1) sequence number of the packet, and (2) the payload. The potential of the signature to compare and identify the same packet is detailed in the later section. Corresponding to this signature, three more fields are also stored in the buffer: (1) Previous hop identity, (2) next hop identity where the packet is forwarded, and (3) Counter, that tells how many times the same packet is received by the node. This information will later be used to get rid of any cycle. The size of the buffer is mainly dependent on the network traffic conditions. However, it is expected to be low due because the sensor nodes sent data either in periodic intervals or upon the occurrence of some event.

Figure 4 : Three sample cycle detection and prevention scenarios.



If the node received the packet whose signature exists in the buffer, then including the previous hop node, two other nodes will also be excluded from the

selection of the next hop process: 1) the node from which last time the packet was received the node from which last time the packet was forwarded. If the same packet is received three times by the same node then the packet will be dropped. Three sample scenarios of the loop creation, detection and prevention are shown in Figure 4. Creation of loops and traversing of the packets in the backward direction is not a completely negative effect. Rather, it provides positive effects in terms of strengthening the route and source location privacy, because these effects will helps to increase the safety period, which is the time for an adversary to reach at the source node.

Identity Privacy: Whenever a node receives the packet *p* from the source node or en-route node then the receiving node will replace the previous hop's identity *prevhop* contained in the packet with its own.After that, the node will get the next forwarding node *nexthop* and update the header of the packet *p* = *{prevhop, nexthop, payload}*. After modification of the two header fields, the node will forward the packet.In this way, all the intermediate forwarding nodes replace the source and next hop's identity contained in the packet *p*. This process will go on until the packet reaches the base station.

Location Privacy: The neighboring nodes which are in each other's radio range can easily approximate the location of each other by measuring the received signal strength and the angle of arrival.If the adversary is within the range of the source node, then adversary can easily estimate the location of the source. Once the packet has crossed the radio range of the original source node, then becomes very difficult for an attacker to estimate the location of the node either in terms of the physical distance or in terms of the number of hops of an original source node. The main reason for this is that the path selection is random and packets are forwarded by only trusted nodes which only contain the information of the last and the next hop.

c) Reliable Identity, Route, and Location Privacy (r-IRL)

It is also possible that some applications require more reliability in terms of packet reach-ability; and the packet could be dropped due to either network congestion or malicious behavior of an en-route node. Thus, in order to achieve more reliability, the packet should be forwarded from multiple paths simultaneously, which will give trustworthiness in the sense that at least the packet should reach the base station by any one of the paths, although, this may increase some communication overhead. Our reliable IRL (r-IRL) algorithm is the extended version of our proposed IRL algorithm, in which we introduce one more parameter, reliability *r*. The source node *i* will multi-cast a packet to all *r* randomly selected neighboring trusted nodes that are in the forward direction. If there are no adequate trusted nodes present in the forward direction, then it will select the remaining trusted nodes from the backward direction. The rest of the mechanism of the r-IRL algorithm is the same as the IRL algorithm.

d) Data Privacy

The payload contains the identity of the source node (IDx) and the actual data (d). Identity is encrypted with the public key $(k+bs)$ of the base station and data is encrypted with the secret key (kx,bs) shared between the sender node and the BS. Both are appended with the payload as shown below:

$$Payload = [E(IDx, k+ bs), E(d, kx, bs)]$$

If we assume that the adversary knows the range of identities assigned to the sensor nodes, public key of the base station and information about cipher algorithm used in the network, an adversary can then successfully obtain the identity of the source by performing simple brute-force search attack by comparing the pattern of encrypted identity with a known range of identities. Therefore in order to provide protection against brute-force search attack, we append a random number (Rn) (equivalent to the size of identity) with the identity of a node and then perform encryption. Now the payload is:

$$Payload = [E(IDx||Rn, k+bs), E(d, kx, bs)]$$

Where // is the append operation. Inclusion of random number may introduce additional computational overhead. However, the amount of overhead is mainly dependent on random number generation technique. Recently, very nice random generation techniques have been specially designed for low power sensor networks, such as. These techniques could be used to generate random number for each packet. Also, overall computational overhead is dependent on the number of packets generated by the sensor nodes.

Our proposed data privacy approach provides several benefits. Firstly, data secrecy is achieved in the presence of identity anonymity. This feature is not available in earlier proposed privacy schemes. Secondly, the base station will receive both the identity of the actual source node and message authentication. If the packet has been successfully decrypted with the shared secret key, it means that packet is received from genuine sensor node.

III. Analysis and Evaluation

a) Energy Consumption Analysis

This section, shows the efficiency of our routing strategies with existing schemes. Energy is computed based on the communication overhead (including transmission and reception cost, path length) introduced by our proposed routing protocols and compared it with other existing schemes.

Table 4 : Simulation parameters

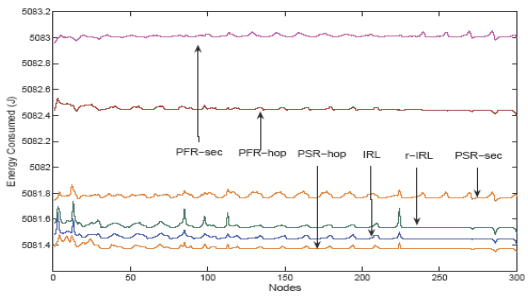
Network specific	Number of nodes	300
	Distance b/w nodes	50 units
	Mobility of nodes	zero
Node specific	Sensor node's Initial battery	1 × 106J
	Power consumption for trans.	1.6W
	Power consumption for recv.	1.2 W
	Idle power consumption	1.15W
	Carrier sense threshold	3.65e−10W
	Receive power threshold	1.55e−11W
	Frequency	9.14e8
	Trans. & Recv. antenna gain	1.0
Protocol & Application specific	Application	CBR
	Reliability param. *r* for r-IRL	3
	hwalk param. for PFR & PSR	10

The proposed paper has implemented our IRL and r-IRL routing schemes on Sensor Network Simulator and Emulator (SENSE).At the application layer we used constant bit rate component (CBR) that generate constant traffic during simulation between randomly selected source node(s) and the base station. For the simplicity, assume that both sensor nodes and the base station are static. Network consists of 300 sensor nodes that are organized into 15 by 20 grid manner.

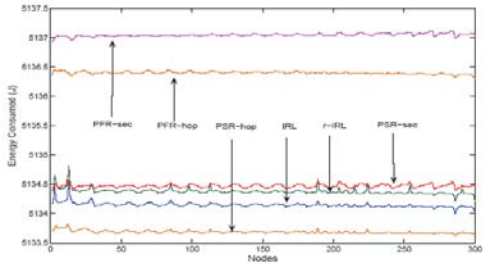
Comparison of proposed IRL and r-IRL algorithms with the four variations of phantom routing schemes that are:

1. Phantom single path routing scheme with hop-based approach (PSR-hop).
2. Phantom single path routing scheme with sector-based approach (PSR-sec).
3. Phantom flood routing scheme with hop-based approach (PFR-hop).
4. Phantom flood routing scheme with sector-based approach (PFR-sec).

Figure 6 : Energy consumption analysis: simulation time: 5,000.



(a) Source node 5

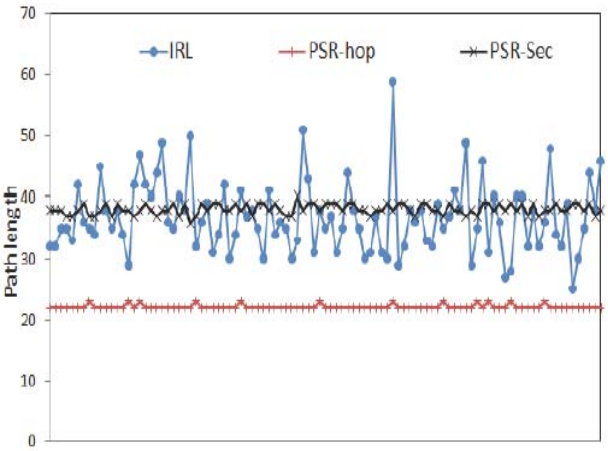


(b) Source node 10

The energy consumption analysis with different scenarios are shown in Figure 6. For the r-IRL scheme we select r = 3, which means a single packet will reach the destination via three different routes simultaneously. For phantom routing schemes, we select parameter $hwalk$=10 (as recommended. Figure 6 clearly indicates that, the IRL and r-IRL schemes consume less energy as compared to the PSR-sec, PFR-hop and PFR-sec schemes but slightly consume higher energy as compared to the PSR-hop scheme. This is due to the fact that the IRL and r-IRL algorithms provides more path diversity and packets sometimes took longer paths.

Our proposed routing strategies (IRL and r-IRL) have both features. Because of the concept of *direction* (Section 3.1), proposed schemes provide more length variation and because of the *randomness* (Section 3.2) proposed schemes provide high path variation. Incorporation of both features offer high path diversity.

Figure 7 : Path diversity of privacy schemes.



In order to analyze the path diversity behavior, assume 300 sensor nodes in a 10 by 30 grid manner. In the simulation, a single source node (ID: 224) generates 100 data packets for the base station. Figure 7 shows the path diversity (in terms of path length) of the IRL, PSR-hop and PSR-sec schemes.

The average path taken by the PSR-hop, IRL and PSR-sec is 22.12, 36.81 and 38.17, respectively. It indicates that the IRL scheme incurs more delay as compared with the PSR-hop scheme and less delay as compared with the PSR-sec scheme. This figure also indicates that the IRL scheme has more path variation as

compared with the other schemes, which creates more difficulties for the adversary to trace back the source from the captured packets.

Figure 7 also shows that some packets took longer paths in the IRL scheme as compared with others. This is due to the fact that the source or en-route node did not find any trusted node in its forward direction, so the packet is relayed back in the backward direction.

Figure 8 shows the result of 100 simulation runs in each node has equal probability to be trusted and un-trusted. It shows that, as the neighborhood size increases, the probability of the packet to move in the backward direction decreases sharply.

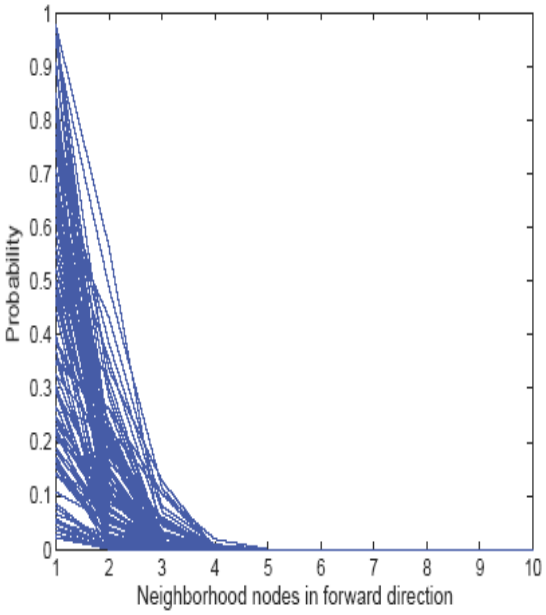


Figure 8 : Probability of a packet to move in the backward direction.

IV. Conclusions and Future Work

Existing privacy schemes of WSNs only provides partial network level privacy. Providing full network level privacy is a critical and challenging issue due to the constraints imposed by the sensor nodes (e.g.,energy, memory and computation power), sensor network (e.g., mobility and topology) and QoS issues (e.g., packet reach-ability and timeliness). Therefore, in this paper we proposed the first full network level privacy solution that is composed of two new identity, route and location privacy algorithms and data privacy mechanism. Our solutions provide additional trustworthiness and reliability at modest cost of energy and memory. Future work, will evaluate proposed schemes from the perspective of computation cost that is required to perform encryption and random number generation.

Bibliography

1. Wood, A.D.; Fang, L.; Stankovic, J.A.; He, T. SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks. In Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, 2006; pp. 35–48.
2. Kamat, P.; Zhang, Y.; Trappe, W.; Ozturk, C. Enhancing Source-Location Privacy in Sensor Network Routing. In Proceedings of the 25th IEEE International conference on Distributed Computing Systems, Columbus, OH, USA, 2005; pp. 599–608.
3. Misra, S.; Xue, G. Efficient Anonymity Schemes for Clustered Wireless Sensor Networks. Int. J. Sens. Netw. 2006.
4. Habitat monitoring on Great Duck Island (Maine, USA), 2002. Available online: http://ucberkeley.
5. Ozturk, C.; Zhang, Y.; Trappe,W. Source-Location Privacy in Energy-Constrained Sensor Network Routing. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks, Washington, DC, WA, USA, 2004; pp. 88–93.
6. Xi, Y.; Schwiebert, L.; Shi, W.Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks. In *Proceedings of Parallel and Distributed Processing Symposium (IPDPS2006)*, Rhodes Island, Greece.
7. Capone, A.; Pizziniaco, L.; Filippini, I.; de la Fuente, M.G. SiFT: An Efficient Method for Trajectory Based Forwarding. In Proceedings of International Symposium on Wireless Communication Systems, Siena, Italy.
8. Zorzi, M.; Rao, R.R. Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Energy and Latency Perfor-mance. IEEE Tran. Mob. Comput. 2003.
9. Blum, B.; He, T.; Son, S.; Stankovic, J. IGF: A State-Free Robust Comm-unication Protocol for Wireless Sensor Networks; Technical Report CS-2003-11; Department of Computer Science, University of Virginia, USA, 2003.
10. Barbeau, M.; Kranakis, E.; Krizanc, D.; Morin, P. Improving Distance Based Geographic Location Techniques in Sensor Networks. In Proceedings of 3rd International Conference on Ad Hoc Networks and Wireless, Vancouver, British Columbia, 2004.
11. RYU, J.; Kim, S.G.; Choi, H.H.; An, S.S.; Ahn, S.Y.; Kim, B.J. Method and System for Locating Sensor Node in Sensor Network Using Transmit Power Control. U.S. Patent Application: 2009/0128298 A1.
12. Barbeau, M.; Kranakis, E.; Krizanc, D; Morin, P. Improving Distance Based Geographic Location Techniques in Sensor Networks. In Proceedings of 3rd International Conference on Ad Hoc Networks and Wireless, Vancouver, British Columbia, 2004.

13. Gaubatz, G.; Kaps, J.-P.; Sunar, B. Public Key Cryptography in Sensor Networks-Revisited. Lect. Note. Comput. Sci. 2006, 3313, pp. 2–18.
14. Lopez, J. Unleashing Public-Key Cryptography inWireless Sensor Networks. J. Comput. Security 2006.
15. Armenia, S.; Morabito, G.; Palazzo, S. Analysis of Location Privacy /Energy Efficiency Tradeoffs in Wireless Sensor Networks. In IFIP-Networking 2007.

This page is intentionally left blank