Network Level Privacy for Wireless Sensor Networks

Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Sungyoung Lee*, Young-Jae Song
Dept. of Comp. Eng., Kyung Hee University, Global Campus, Suwon, Korea.
{riaz, hassan, dauriol, sylee}@oslab.khu.ac.kr, yjsong@khu.ac.kr

Heejo Lee
Dept. of Comp. Sci. & Eng., Korea University, Seoul, Korea.
heejo@korea.ac.kr

Abstract

Full network level privacy spectrum comprises of identity, route, location and data privacy. Existing privacy schemes of wireless sensor networks only provide partial network level privacy. Providing full network level privacy is a critical and challenging problem due to the constraints imposed by the sensor nodes, sensor networks and QoS issues. In this paper, we propose full network level privacy solution that addresses this problem. This solution comprises of Identity, Route and Location (IRL) privacy algorithm and data privacy mechanism, that collectively provides protection against privacy disclosure attacks such as eavesdropping and hop-by-hop trace back attacks.

1 Introduction

Networks are comprised of three dynamic entities: nodes, routes and packets. Based on these dynamic entities, full network level privacy has often been categorized into four sub-categories: 1) Sender node identity privacy: no intermediate nodes 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 nodes 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 nodes and adversary can predict the information about the complete path (from source to destination). 4) Data packet privacy: no nodes can be able to see the information inside in a payload of the data packet except the source and destination. In WSNs, destination node is usually the sink node or the base station that is known to all the nodes in the network. That is why identity and location privacy of the destination node is not considered here.

Existing privacy schemes such as [8, 4, 7, 11, 12] that have specifically been proposed for WSNs only provide partial network level privacy. Providing a full network level privacy spectrum 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 reachability, and trustworthiness).

In order to achieve this goal, we incorporate basic design features from related research fields such as geographic routing and cryptographic systems. We propose the first full network level privacy solution for WSNs. Our contribution lies in following features. A new Identity, Route and Location (IRL) privacy algorithm is proposed that ensures the anonymity of source node's identity and location from the adversary. It also gives assurance that the packets will reach their destination by passing through only trusted intermediate nodes. A new data privacy mechanism is proposed, which is unique in the sense that it provides data secrecy and packet authentication in the presence of identity anonymity. Also, our solutions collectively provides protection against various privacy disclosure attacks such as eavesdropping and hop-by-hop trace back attacks.

The remainder of the paper is organized as follows: Section 2 contains related work, Section 3 describes the proposed privacy scheme, Section 4 consists of security resiliency analysis, and Section 5 concludes the paper and gives directions of future work.

*Corresponding author.

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)"(IITA-2008-C1090-0801-0002) and by the MIC(Ministry of Information and Communication), Korea, Under the ITFSIP(IT Foreign Specialist Inviting Program) supervised by the IITA (C1012-0801-0003). Also, this work is financially supported by the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and Energy (MOCIE) and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency.

978-0-7695-3324-7/08 $25.00 © 2008 IEEE
DOI 10.1109/IAS.2008.36

2 Related Work

C. Ozturk et al. [8] proposed a phantom routing scheme for WSNs, which helps to prevent the location of a source from the attacker. In this scheme, each message reaches the destination in two phases: 1) a walking phase, in which the message is unicasted in a random fashion with in first h_{walk} hops, 2) after that, the message is flooded using the baseline flooding technique. The major advantage of their scheme is the source location privacy protection, which improves as the network size and intensity increases because of high path diversity. But on the other hand, if the network size increases the flooding phase will consume more energy. This scheme does not provide identity privacy. Also, it is unable to provide data secrecy in the presence of identity privacy.

P. Kamat et al. [4] proposed a phantom single-path routing scheme that works in a similar fashion as the original phantom routing scheme [8]. The major difference between these two schemes is that after the walking phase, a packet will be forwarded to the destination via a single path routing strategy such as the shortest path routing mechanism. This scheme consumes less energy and requires slightly higher memory as compared to first one. This scheme also do not provide identity privacy. Also, it is unable to provide data secrecy in the presence of identity privacy.

S. Misra and G. Xue [7] proposed two schemes: Simple Anonymity Scheme (SAS) and Cryptographic Anonymity Scheme (CAS) for establishing anonymity in clustered WSNs. The SAS scheme use dynamic pseudonyms instead of true identity during communications. Each sensor node needs to store a given range of pseudonyms that are non-contiguous. Therefore, the SAS scheme is not memory efficient. On the other hand, the CAS scheme uses keyed hash functions to generate pseudonyms. This scheme is memory efficient as compare to the SAS but it requires more computation power. The authors does not propose any routing scheme. Sender node may always send packets to the destination via shortest path. In that case, for an adversary who is capable of performing hop-by-hop trace back (with the help of direction information) can find out the location of the source node.

A. D. Wood et al. [11] have proposed a configurable secure routing protocol family called Secure Implicit Geographic Forwarding (SIGF) for WSNs. The SIGF is based on the Implicit Geographic Forwarding (IGF) protocol [1] in which a packet is forwarded to the node that lies within the region of 60° sextant, centered on the direct line from the sender to the destination. The SIGF protocol provides some aspects of networks privacy such as data, route and location privacy. However it does not provide identity privacy. Another, limitation of the SIGF protocol is that, when there is no trusted node within a forwarding area (assuming 60° sextant), it will forward the packet to a un-trusted node. So, the reliability of the path is affected.

Y. Xi et al. [12] proposed a Greedy Random Walk (GROW) scheme for preserving location of the source node. This scheme works in two phases. In a first phase, the sink node will set up a path through random walk with a node that act as a receptor. Then the source node will forward the packet towards the receptor in a random walk manner. Once the packet reaches at the receptor, it will forwards the packet to the sink node through the pre-established path. Here receptor is acting a central point between the sink and the source node for every communication session. Criteria of selecting a trustworthy receptor is essential that is not defined.

3 Proposed Scheme

3.1 Network Model and Assumptions

WSN is composed of large number of resource-constraint sensor nodes that are densely deployed in an environment. Links are bidirectional. For scalability reason, it is assumed that no sensor node needs to know the global network topology, except that it must know the geographical location of its own, its neighboring nodes and the base station. We also assumed that each sensor nodes stores two keys. First, unique secret key [9, 5] that is shared between each sensor node and the base station (BS). These keys could be periodically updated. Second, public key of the BS. Sensor nodes do not require their own public and private keys, because computation cost of a public and private keys at the sensor node is very high. It is also assumed that sensor nodes are capable of performing encryption and decryption of the data by using at least two cipher algorithms (one symmetric and other asymmetric). This provides an additional layer of security.

3.2 Concepts and Definitions

The first notion used in our algorithm 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 (B_r), 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 3.3. A node x classifies its neighboring node y in following fashion:

$$C_{x,y} = \begin{cases} F & \frac{-\pi}{2} \leq \theta \leq \frac{\pi}{2} \\ B_r & \frac{\pi}{2} < \theta \leq \frac{5\pi}{6} \\ B_m & \frac{5\pi}{6} < \theta \leq \frac{7\pi}{6} \\ B_l & \frac{7\pi}{6} < \theta < \frac{3\pi}{2} \end{cases} \quad (1)$$

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.

The second notion used in our algorithm is that of trust. Definition of a trust here is based on our another paper [10] and is provided here as a gist in simplified form.

Trust is considered as a measure of node reliability [13, 6] which is evaluated based on the direct observations of the neighboring nodes' behavior. Direct observations represent the number of successful and unsuccessful interactions, which are calculated based on the control packets received at the link layer of the node. For example, a sender will consider interaction as a successful one if the sender receives assurance that the packet is successfully received by the neighbor node and it has forwarded it 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 using enhanced passive acknowledgment (PACK) by overhearing the transmission of a next hop on the route, since they are within radio range [2]. If the sender node does not overhear the retransmission of the packet within a predefined threshold time from its neighboring node or 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 an unsuccessful one. Based on these successful and unsuccessful interactions node x can calculate the trust value of node y in following fashion:

$$T_{x,y} = \left[100 \left(\frac{S_{x,y}}{S_{x,y} + U_{x,y}} \right) \left(1 - \frac{1}{S_{x,y} + 1} \right) \right] \quad (2)$$

where [.] is the nearest integer function, $S_{x,y}$ is the total number of successful interactions of node x with y and $U_{x,y}$ is the total number of unsuccessful interactions of node x with y during last session. After the end of each session the record of successful and unsuccessful interactions will replace with the new one. The expression $\left(1 - \frac{1}{S_{x,y}+1}\right)$ in the above approaches 1 rapidly with an increase in the number of successful interactions. In order to balance this increase in the trust value with the increasing number of unsuccessful interactions, we multiply the expression with factor $\left(\frac{S_{x,y}}{S_{x,y}+U_{x,y}}\right)$, which indicates the percentage of successful interactions among the total interactions. Based on the trust value each node classifies its neighboring nodes into two categories in following fashion:

$$C(T_{x,y}) = \begin{cases} \text{trusted} & 50 \leq T_{x,y} = 100 \\ \text{untrusted} & 0 \leq T_{x,y} < 50 \end{cases} \quad (3)$$

We have used both these notions (direction and trust) in order to select reliable secure paths for achieving robust route privacy.

Algorithm 3.1 IRL - Routing

```
1: prev_hop ← ∅; next_hop ← ∅;
2: if M(t_f) ≠ ∅ then
3:    next_hop(k) = Rand(M(t_f));
4: else
5:    if source_node = true then
6:       if M(t_{B_r}) ∪ M(t_{B_l}) ≠ ∅ then
7:          next_hop(k) = Rand(M(t_{B_r}) ∪ M(t_{B_l}));
8:       else if M(t_{B_m}) ≠ ∅ then
9:          next_hop(k) = Rand(M(t_{B_m}));
10:      else
11:         Drop packet and Exit;
12:      end if
13:   else
14:      if packet came from B_{r|l|m} then
15:         if M(t_{B_{l|r|r}}) ∪ M(t_{B_{m|m|l}}) ≠ ∅ then
16:            next_hop(k)= Rand(M(t_{B_{l|r|r}}) ∪ M(t_{B_{m|m|l}}));
17:         else if M(t_{B_{r|l|m}}) ≠ ∅ then
18:            next_hop(k) = Rand(M(t_{B_{r|l|m}})\{prev_hop});
19:         else
20:            Drop packet and Exit;
21:         end if
22:      end if
23:   end if
24: end if
25: Set prev_hop = my_id;
26: Form pkt p = {prev_hop, next_hop, seqID, payload};
27: Forward packet to next_hop;
28: Set timer Δt = D / d_{next_hop} × t;
29: while Δt = true do
30:    Signature remains in buffer;
31: end while
32: Signature removed from buffer;
```

3.3 Identity, Route, and Location Privacy

Our 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; out of which, t nodes are trusted. So, $0 \leq t \leq m$ and $M(t) = M(t_f) \cup M(t_{B_r}) \cup M(t_{B_l}) \cup M(t_{B_m})$. Here $M(t_f)$, $M(t_{B_r})$, $M(t_{B_l})$, and $M(t_{B_m})$ represent the set of trusted neighboring nodes that are in the forward, right backward, left backward, and middle backward directions, respectively. These neighbor sets are initialized and updated whenever change occur in the 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 (Algorithm 3.1) of IRL algorithm is called. In order

to forward a packet, the node will first check the set $M(t_f)$ of trusted forwarded nodes (Line 2). If it is not empty, then the node i will randomly select one node as a next hop (Line 3) from the set $M(t_f)$ and forward the packet towards it (Lines 25:32). Before forwarding the packet, node i will save the signature of the packet, which consists of sequence ID and payload, in the buffer. This signature remains in the buffer for Δt time, that is:

$$\Delta t = 2\left(\frac{D}{d} \times p_t\right) \tag{4}$$

where D is the distance between forwarding node and the base station, d is the distance between forwarding node and the next hop, and p_t is the propagation transfer time between forwarding node and the next hop. This signature will help to detect cycle.

If the forwarding set $M(t_f)$ is empty, then the node i will first check whether it is source node or an en-route node (Line 5). If the forwarding node itself is the actual source node then the node i will randomly select one node from the set containing list of the trusted nodes that are in the right as well as in the left backward sets (Lines 6:7) and forward the packet towards it (Lines 25:32). If there is no trusted node in the right and left backward sets then it will randomly select one trusted node from the middle backward set (Lines 8:9) and forward packet toward it (Lines 25:32). This process will go on until the packet reaches the base station. If there is no trusted node in the forward as well as in the whole backward direction then the packet will be dropped (Line 11).

If the forwarding node is an en-route node and has no trusted node in the the forward direction, then it will first check the sender of a packet belongs to which set. For example, if the packet, forwarded by a node, belongs to the right backward set (Line 14), then it will first check whether other two backward sets (left and middle) contain any trusted nodes (Line 15) or not. If yes, it will randomly select one node from the those sets (Line 16) and forward packet towards it (Lines 25:32). If there is no trusted node in those two sets (Line 17) then the node will randomly select trusted node from the right backward set ($M(t_{B_r})$) excluding the one from where the node i received the packet (Line 18) and forward the packet towards it (Lines 25:32). Similar operations will be performed, if the packet, forwarded by a node, belongs to the left or middle backward sets.

Identity Privacy: Whenever a node receives the packet p from the source node then the receiving node will replace the previous hop's identity $prev_{hop}$ contained in the packet with its own (Line 25). After that, the node will get the next forwarding node $next_{hop}$ (as described earlier) and update the header of the packet $p = \{prev_{hop}, next_{hop}, \text{payload}\}$ (Line 26). After modification of the two header fields, the node will forward the packet (Line 27). 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 [3]. 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 (due to randomness) 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.

3.4 Data Privacy

The payload contains identity of the source node (ID_x) 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 ($k_{x,bs}$) shared between the sender node and the BS. Both are appended with the payload as shown below:

$$\text{payload} = [E(ID_x, k_{bs}), E(d, k_{x,bs})] \tag{5}$$

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. Then, an adversary can successfully able to get the identity of the source by performing simple brute-force search attack by comparing the pattern of encrypted identity with the range of identities he knows. Therefore in order to provide protection against brute-force search attack, we append a random number (R_n) (equivalent to the size of identity) with the identity of a node and then perform encryption. Now the payload is:

$$\text{payload} = [E(ID_x||R_n, k_{bs}), E(d, k_{x,bs})] \tag{6}$$

where $||$ is the append operation.

This approach provides several benefits such as: 1) Data secrecy is achieved in the presence of identity anonymity. 2) Base Station will not only able to get the identity of actual source node but also it provide message authentication.

4 Security Resiliency Analysis

Suppose we have an adversary $\mathcal{A}$ whose wish is to defeat our privacy protocols and guess the original source node. We will distinguish between two kinds of nodes. A source node is the node which is the original sender of a packet q and a forwarding node is a node which forwards a packet to another node until it reaches the destination. Hence the source node is also a forwarding node. The adversary's goal

is to find out the source node. This analysis assumes that we are using IRL algorithm including our proposed data privacy mechanism. So if the adversary sees a packet, it will trivially know the identity of the last forwarding node.

We will deal with separate cases. Case 1 is when the adversary is close to the base station and can eavesdrop on any packet received by the base station. Case 2 deals with the case when the adversary can see any packet within the radio range of a particular node. Case 3 extends this to two or more nodes.

An adversary will try to solve the following problem: Given a packet q and a subset of nodes N', find out the sender node s. In other words the algorithm for the adversary takes two inputs and outputs a node s'; Namely $\mathcal{A}(q, N') = s'$. If $s' = s$, the adversary wins and is successful in defeating our protocol. We have to find: $P(\mathcal{A}(q, N') = s)$ that is the probability of an adversary to find out the sender node.

Notations and definitions: Denote a generic node by m. The set of neighbors of m is denoted by N_m, which also includes m itself. The number of forward and backward nodes of m is denoted by m_f and m_b respectively. If a node a is a backward node of m, then we denote it as $a \rightarrow m$. We say that a node a is in the backward set of node m, if $a \rightarrow a_1 \rightarrow \ldots a_r \rightarrow m$, for some nodes $a_1, \ldots a_r$ where $r \geq 0$. For compact notation we will denote this as $a \rightarrow^r m$, if the IDs of the intermediate nodes are not significant. We will also use the notation $\rightarrow^r m$ to denote a generic node, who is r links (hops) away from m. Define the backward set C_m of m as $C_m = \{a | a \rightarrow^r m, r \geq 0\}$, that is the set of all the possible nodes such that they have a forward link to m. Denote the base station as B. It will also be seen as another node. Let the total number of nodes in the network excluding the base station be N. We will use the term "adversary is in possession of a node" to indicate that the adversary can passively listen to any communication within the radio range of that node.

Claim 1: Suppose A is in possession of B. Let B_b be the number of backward nodes of the base station (nodes one hop away from the base station). Then for any packet q received by B:

$$P\left(\mathcal{A}\left(q, N\right) = s\right) = \frac{B_b + 1}{N} \tag{7}$$

Proof: The adversary can always know the ID of the last forwarding node. Let B_b be the number of backward nodes to the base station. The packet could only have come from one of the nodes in $N_B - \{B\}$ (which only contains backward nodes to B). Since the nodes are just a hop away from the BS, so they will not send the packet to another node. Hence for large N we have:

$$\begin{aligned} P\left(\mathcal{A}\left(q, N\right) = s\right) = P\left(\mathcal{A}\left(q, N\right) = s | s \in N_B - \{B\}\right) \times \\ P\left(s \in N_B - \{B\}\right) + \\ P\left(\mathcal{A}\left(q, N\right) = s | s \notin N_B - \{B\}\right) P\left(s \notin N_B - \{B\}\right) \\ = 1 \cdot \frac{B_b}{N} + \frac{1}{N - B_b - 1}\left(1 - \frac{B_b}{N}\right) \\ \approx \frac{B_b}{N} + \frac{1}{N - B_b}\left(1 - \frac{B_b}{N}\right) = \frac{B_b + 1}{N} \end{aligned}$$

□

Now let us assume that $\mathcal{A}$ is in possession of a node m in the network. Let us exclude the possibility that a packet will be sent backwards during its course to the base station, since the probability of it happening is very small. Furthermore even if we consider it, it will decrease the probability of success of the adversary since there would be more possible nodes. Thus in this scenario our result would be like an upper bound on the adversary's limitations.

Claim 2: Suppose $\mathcal{A}$ is in possession of a node m. Let $c = |C_{\rightarrow^2 m}|$ denote the number of backward nodes in backward set $C_{\rightarrow^2 m}$ of some node $\rightarrow^2 m$. Then,

$$P\left(\mathcal{A}\left(q, N\right) = s\right) = \frac{m_f + m_b + 1}{N} + \frac{1}{c+1}\left(1 - \frac{m_f + m_b + 1}{N}\right) \tag{8}$$

Proof: Since the adversary is in possession of a node m, it knows its backward and forward nodes. Furthermore, if any of these nodes including the node m itself is the sender of a packet q, then the adversary will know. This is true since the adversary can see all the incoming packets to the node m and to its neighbor nodes (the forward and the backward nodes). Thus it can see if the payload of q is not equal to the payload of any q' being received by these nodes in a given interval of time. If this is the case, then the adversary will know the sender.

Now if none of the nodes in N_m are the senders, then the packet was forwarded by a node i which is two hops away from m. The adversary knows the ID of that node through the packet q. Thus the adversary makes a list of all the possible backward nodes in the backward set of i. Let that number be denoted by c. Notice that node i could also be the possible sender. Hence the total number of possible senders would be $c + 1$. We have:

$$\begin{aligned} P\left(\mathcal{A}\left(q, N\right) = s\right) = P\left(\mathcal{A}\left(q, N\right) = s | s \in N_m\right) P\left(s \in N_m\right) \\ + P\left(\mathcal{A}\left(q, N\right) = s | s \notin N_m\right) P\left(s \notin N_m\right) \\ = \frac{m_f + m_b + 1}{N} + \frac{1}{c+1}\left(1 - \frac{m_f + m_b + 1}{N}\right) \end{aligned}$$

□

Now, suppose the adversary is in possession of two nodes at the same time m_1 and m_2. We can safely assume that $N_{m_1} \cap N_{m_2} = \varphi$, since it would be more advantageous to the adversary to cover nodes with non overlapping radio ranges. The adversary will always know whenever any node in N_{m_1} or N_{m_2} is the sender of a packet. How about the case when they are not the senders? There could be two

possible cases. Without loss of generality, first assume that $m_2 \in C_{m_1}$. If the packet q was received by some node in N_{m_1} and was received by some node in N_{m_2} before, then the adversary had already checked it when the packet was sent to a node in N_{m_1}. Thus the adversary need only check packets received in N_{m_1} which were not received by N_{m_2}. In this case, the sender cannot be in N_{m_2}. In any case, the adversary has to find out the backward sets of $\rightarrow^2 m_1$ or $\rightarrow^2 m_2$, depending on where the packet was received. Since the network traffic is uniformly distributed, therefore the probability of a packet being received at the two sets is the same. In case $m_2 \notin C_{m_1}$, then the adversary has no real advantage except that it can see packets at two disjoint locations in the network. Thus we only state the case when $m_2 \in C_{m_1}$. We have the following result:

Claim 3: Suppose the adversary is in possession of two nodes m_1 and m_2. Assume further that $m_2 \in C_{m_1}$. Let $c_1 = |C_{\rightarrow^2 m_1}|$ and $c_2 = |C_{\rightarrow^2 m_2}|$ then:

$$P(\mathcal{A}(q,N) = s) = \frac{|N_{m_1}|+|N_{m_2}|}{N} + \frac{1}{2}\left(\frac{1}{c_1+1-|N_{m_2}|} + \frac{1}{c_2+1}\right)\left(1 - \frac{|N_{m_1}|+|N_{m_2}|}{N}\right) \quad (9)$$

In general, we have:

Claim 4: Let us assume that $\mathcal{A}$ is in possession of k nodes $m_k \rightarrow^{r_1} \cdots \rightarrow^{r_{k-2}} m_2 \rightarrow^{r_{k-1}} m_1$ and let m_f and m_b denote the average number of forward and backward nodes averaged over all the k nodes. Let $t = m_f + m_b + 1$. For $1 \leq i \leq k$, let $c_i = |C_{\rightarrow^2 m_i}|$, then:

$$P(\mathcal{A}(q,N) = s) = \frac{kt}{N} + \frac{1}{k}\left(\frac{1}{c_1+1-(k-1)t} + \frac{1}{c_2+1-(k-2)t} \cdots + \frac{1}{c_k+1}\right)\left(1 - \frac{kt}{N}\right) \quad (10)$$

Observations: The probability is lowest when the adversary is actually at the base station. If the adversary has more nodes in possession, the probability increases linearly, with more success rate when the nodes are actually connected. This also shows that if a packet originates from any node which does not have a backward node, the adversary will always know the sender.

5 Conclusion 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 first full network level privacy solution. This solution additionally provides trustworthiness and reliability. We also proved analytically that our solution provides protection against an adversary who is capable of performing privacy disclosure attacks. In future, we will do memory, energy and time delay analysis and evaluation of our proposed solution.

References

[1] B. Blum, T. He, S. Son, and J. Stankovic. IGF: A state-free robust communication protocol for wireless sensor networks. *Tech. Rep. CS-2003-11, Dept. of Comp. Sci. University of Virginia, USA*, 2003.

[2] S. Buchegger and J.-Y. L. Boudec. A robust reputation system for peer-to-peer and mobile ad-hoc networks. In *Proc. of P2PEcon*, Cambridge MA,USA, Jun 2004.

[3] A. Durresi, V. Paruchuri, M. Durresi, and L. Barolli. Anonymous routing for mobile wireless ad hoc networks. *Int. J. of Distributed Sensor Networks*, 3:105–117, 2007.

[4] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In *Proc. of 25^{th} IEEE Int. conf. on Distributed Computing Systems*, pages 599–608, Columbus, Ohio, USA, Jun 2005.

[5] C. Karlof, N. Sastry, and D. Wagner. TinySec: a link layer security architecture for wireless sensor networks. In *Proc. of 2^{nd} Int. Conf. on Embedded networked sensor systems*, pages 162–175, Baltimore, MD, USA, Nov. 2004.

[6] K. Liu, N. Abu-Ghazaleh, and K.-D. Kang. Location verification and trust management for resilient geographic routing. *J. of Parallel and Dist. Computing*, 67:215–228, 2007.

[7] S. Misra and G. Xue. Efficient anonymity schemes for clustered wireless sensor networks. *Int. J. of Sensor Networks*, 1(1/2):50–63, 2006.

[8] C. Ozturk, Y. Zhang, and W. Trappe. Source-location privacy in energy-constrained sensor network routing. In *Proc. of 2^{nd} ACM workshop on Security of Ad hoc and Sensor Networks*, pages 88–93, DC, USA, Oct 2004.

[9] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. SPINS: security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, 2002.

[10] R. A. Shaikh, H. Jameel, B. J.d'Auriol, H. Lee, S. Lee, and Y.-J. Song. Group-based trust management scheme for clustered wireless sensor networks. In *Submitted for publication*.

[11] A. D. Wood, L. Fang, J. A. Stankovic, and T. He. SIGF: a family of configurable, secure routing protocols for wireless sensor networks. In *Proc. of 4^{th} ACM workshop on Security of ad hoc and sensor networks*, pages 35–48, Alexandria, Virginia, USA, 2006.

[12] Y. Xi, L. Schwiebert, and W. Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In *Proc. of IPDPS 2006*, Rhodes Island, Greece, Apr 2006.

[13] Z. Yao, D. Kim, and Y. Doh. PLUS: Parameterized and localized trust management scheme for sensor networks security. In *Proc. of the 3^{rd} IEEE Conf. on Mobile Ad-hoc and Sensor Systems*, pages 437–446, Vancouver, Canada, Oct 2006.