On the Tradeoff Between Privacy and Energy in Wireless Sensor Networks

Sambid Shrestha, Matthew Leeke and Arshad Jhumka
Department of Computer Science
University of Warwick
Coventry, UK, CV4 7AL
{*csugdi, matt, arshad*}*@dcs.warwick.ac.uk*

***Abstract*—Source location privacy is becoming an increasingly important property of some wireless sensor network applications. The fake source technique has been proposed as an approach for handling the source location privacy problem in these situations. However, whilst the efficiency of the fake source techniques is well documented, there are several factors that limit the usefulness of current results: (i) the assumption that fake sources are known *a priori*, (ii) the selection of fake sources based on an prohibitively expensive pre-configuration phase and (iii) the lack of a commonly adopted attacker model. In this paper we address these limitations by investigating the efficiency of the fake source technique with respect to possible implementations, configurations and extensions that do not require a pre-configuration phase or *a priori* knowledge of fake sources. The results presented demonstrate that one possible implementation, in presence of a single attacker, can lead to a decrease in capture ratio of up to 60% when compared with a flooding baseline. In the presence of multiple attackers, the same implementation yields only a 30% decrease in capture ratio with respect to the same baseline. To address this problem we investigate a hybrid technique, known as phantom routing with fake sources, which achieves a corresponding 50% reduction in capture ratio.**

***Keywords*-Wireless Sensor Networks; Fake Sources; Source Location Privacy; Power Consumption; Multiple Attackers**

I. Introduction

Over the last decade the advent of wireless sensor networks has enabled several novel classes of applications, such as monitoring and tracking. In the case of monitoring applications, deployment of these sensor networks will vary from critical applications, such as military, health and asset monitoring, to non-critical applications, such as temperature and humidity control. For critical applications, privacy will be an important property. Due to the fact that wireless sensor networks operate in a broadcast medium, attackers can easily intercept messages and attempt to subvert a system.

The privacy threats that exist for sensor networks can be broadly classified along two dimensions, namely (i) *content-based* privacy threats and (ii) *context-based* privacy threats. Content-based privacy threats relate to threats that are based on the contents of messages, i.e., the threats are against the values generated by the network layers either at the application level (e.g., sensed values) or lower-layer levels (e.g., time-stamps). Context-based privacy threats are based on the context associated with the measurement and transmission of sensed data. Context is a multi-attribute concept that captures several environmental aspects associated with sensed data, such as location and time. While content-based threats are well-understood [10], context-based threats are becoming increasingly important. For content-based threats, nodes launching attacks are often modelled as Byzantine nodes [6], with cryptographic techniques often being used to address these problems [2] [6]. However, cryptographic techniques do not address context-based threats.

One aspect of context that is important in several applications is *location*. Location information can be embedded in a message, but remain inaccessible to an attacker due to encryption of the message. Thus, if location information cannot be directly obtained, then it can be inferred. One important problem for monitoring applications is the problem of *source location* privacy. In this problem, a wireless sensor network is monitoring an asset. The nodes detecting the asset, known as *source nodes*, will periodically send messages to a dedicated node, known as the *sink node*, for data collection. If the location(s) of the source node(s) is compromised, then an attacker can capture the asset.

It is possible to infer location information through various techniques, depending on the power of the attacker. For example, Metha et.al [8] assumes that an attacker has a small wireless network of his own that can capture messages and shows how the location of source nodes can be inferred once messages have been intercepted. In contrast, Kamat et.al [5] assumes a single attacker, who can use the adopted routing protocol to infer the location of a source node. For example, in a military environment, soldiers on surveillance may relay information to a sink. An attacker can intercept these messages and trace them back to their source, thereby compromising the safety of the soldiers. Several techniques to handle the source location privacy problem have been proposed [1] [5] [7] [8] [13]. In this paper we focus on the *fake source* technique. However, current results associated with this technique are of limited relevance, since they make a number of assumptions which limit their practicality: (i) fake sources are known *a priori*, (ii) fake sources are selected based on an prohibitively expensive pre-configuration phase and (iii) no common attacker model is adopted.

To address the described limitations we investigate the efficiency of fake sources with respect to possible imple-

mentations, configurations and extensions. We make several novel contributions: (i) we detail possible implementations of the fake source protocol that circumvents the need for fake sources to be known *a priori*, (ii) we make no undue assumption regarding the capabilities of the sensor nodes, (iii) we investigate the efficiency of fake sources in presence of a distributed eavesdropper, which can possibly have multiple implementations, e.g., using single or multiple attackers, and (iv) we develop a hybrid technique that accounts for multiple attackers. In doing this we present results which show that one possible implementation, in presence of a single attacker, can lead to a decrease in capture ratio of up to 60% when compared with a flooding baseline. In the presence of multiple attackers, the same implementation yields only a 30% decrease in capture ratio over the same baseline. To counteract this problem we apply our hybrid technique, known as phantom routing with fake sources, which achives a corresponding 50% reduction in capture ratio with respect to the same baseline.

A. Paper Structure

This paper is structured as follows: In Section II we provide a survey of related work. In Section III we define the network and attacker models used in the paper. In Section IV we describe the protocols investigated, outlining their key characteristics and the reasoning upon which they are based. In Section V we outline our experimental approach. The results generated are presented and discussed in Section VI. Section VII concludes this paper with a paper summary.

II. Related Work

The problem of source location privacy first appeared around 2004 [5] [9]. Since then, the problem has been addressed using a variety of attacker models and assumptions. These varied attacker models and assumptions have led to the development of many solutions and techniques for enhancing source location privacy. Ozturk et.al [9] investigated the privacy imparted by flooding, and several other techniques such as fake source and phantom routing. A similar investigation was performed by Kamat et.al [5]. Subsequently, a new attack was shown to subvert the technique proposed by Kamat et.al [5], based on the assumption that nodes have access to their location using GPS devices. The most commonly adopted attacker model is a local attacker model, where nodes have only local knowledge. Other approaches have begun to investigate the impact of a global eavesdropper. Under these circumstances it has been shown that, for a fake source protocol where every node in the network acts as a fake source, maximal privacy can be ensured.

Despite the body of work relating to source location privacy in wireless sensor networks, little work has investigated the impact of possible fake source implementations and configuration parameters on source location privacy. This problem in directly addressed in this paper.

III. Models

In this section we detail the system / network and attacker models adopted in this paper.

A. System Model

We define a wireless sensor node as a computing device equipped with a wireless interface and associated with a unique identifier. Communication in wireless sensor networks is typically modelled with a circular communication range centred on the node, and we assume that all nodes have the same communication range, implying that nodes have omni-directional antennas. This assumption contrasts with work that assumes directional antennas [12]. Under this model a node is thought of as able to exchange data with all devices within its communication range. A wireless sensor network is a collection of wireless sensor nodes and is modelled as an undirected graph $G = (V, E)$, where V is a set of N wireless sensor nodes and E is a set of edges or links, each link being a pair of distinct nodes. A link exists between two nodes if they are in each other s communication range. Two nodes $m \in V$ and $n \in V$ are said to be 1-hop neighbours (or neighbours) iff $\{m, n\} \in E$, i.e., m and n are in each other's communication range. We denote by M the set of m's neighbours. The graph $G = (V, E)$ defines the topology of the network. In this paper, we focus on grid-like network topology, i.e., network of size $n * n = N$.

There exists a distinguished node S in the network called a sink, which is responsible for collecting data. Other nodes $v \in V \setminus \{S\}$ can sense data and then route the data to the sink for collection. In general, any node can be a source of sensed data. In this paper, however, we assume that only a subset of nodes can be a source of sensed data. Specifically, from our assumption of grid-like network, we assume nodes on the perimeter of the network to be sources of sensed data.

Sensor nodes route messages to the sink, generally using data aggregation convergecast protocols. It has been previously shown that an attacker can use routing information to launch source-location privacy attacks. It has been also shown that a basic routing strategy like flooding does not have good source location privacy properties [5], and various variants, e.g., use of fake source on top of flooding and directed random walk followed by flooding, have been proposed to improve the privacy provided by a given routing strategy. We assume message content to be encrypted, thus it can only be read by the correct node and not by an attacker.

B. Attacker Model

In this paper an attacker is considered to be a set of sensor nodes. It has been proposed in [3] that the strength of an attacker for wireless sensor can be captured along two main dimensions, namely (i) presence and (ii) actions. For example, presence can be local or global, while examples of actions includes eavesdropping and reprogramming. Using these two dimensions, a lattice of attacker strengths was

developed. Based on this lattice, we consider one type of attacker, namely a *distributed eavesdropping* attacker. There can be different implementations of this type of attacker. For example, such an attacker can be a single mobile person with a sensor node trying to eavesdrop. Another implementation can be multiple persons, each with a sensor node, eavesdropping on the network. In this paper we consider these two possible implementation of a distributed eavesdropper and analyse the impact of a given routing strategy with respect to the attacker implementation. We also assume that the attacker does not have any knowledge of the network, i.e., the attacker does not know the network topology or the adopted routing algorithm. The only knowledge a distributed eavesdropper has is that which is deduced based on the eavesdropping on the network. For example, when a message from a legitimate node within its neighbourhood is received, the sender of that message can be located but the source of the message is not known.

IV. Fake Source Protocols

In this section we describe the fake source technique for providing source location privacy. We abstract away implementation details in order to identify important parameters for any implementation of the technique, as well as presenting the implementations used in this paper.

A. Fake Sources

As its name suggests, the fake source technique involves selecting a subset of nodes to act as fake sources, i.e., to simulate a real source. The current state-of-the-art assumes *a priori* knowledge of these fake sources. However, in practice fake sources have to be chosen during operation. Previous work on fake sources distinguished between temporary fake sources and permanent fake sources [5]. This work concluded that permanent fake sources outperform temporary fake sources. In this paper we focus on permanent fake sources. A permanent fake source is a node that continuously sends network message to simulate a real source for at least the duration of message transmission from the real source.

A real source is characterised by its location and message transmission rate. Any implementation of the fake source technique must investigate the impact of at least these two parameters. It has been argued that better privacy is achieved by having a fake source be a similar distance away from the sink as the real source [5].

B. Fake Source 1 (FS1) Implementation

We assume that real sources uses a flooding protocol to send messages to a sink. The flooding protocol is implemented as follows. The source generates a message and then broadcasts it to every node in its neighbourhood. The general structure of a message is:

$$< text, count, hash, destination, origin, hops >$$

For example, a transmitted message might be:

$$< message, 1, message - 1, -, 121, 0 >$$

In this example, the unique identifier of the source node is 121 and the $destination$ field is empty. When a node receives a message it checks the *count* value and determines whether it is a new message. If this is a new message, the node records the *count* value, increments the hop count and forwards the message. The node will drop any message that it has already been forwarded. Thus, using the flooding protocol, messages generated by the real source is forwarded by each node to the sink. When the sink receives the first such message it broadcasts an away message to each of its neighbours. The away message structure is:

$$< away, 1, away - 1, -, 99, 5 >$$

Here, as a matter of example, the sink id is 99 and the hop distance between the real source and sink is 5. The nodes that receive the away message check if they have received a message from the source with the count value of 1. If they have received such a message, the node reduces the hop count by one and generates a choose message and broadcasts this message to its neighbours. The purpose of this away message is to ensure that only nodes that are further away from the real source forward the choose message.

Each intermediate node that receives the choose message will generate a random number R. If R is greater than a given threshold τ, the node will decrement the hop count and forward the message to its neighbours. Further, when a node receives a choose message that has a hop-count value of 0, the node generates its random number R. If R is greater than τ, then the node becomes a fake source, and starts generating messages, which we call fake messages. The structure of the fake messages generated by a fake source is:

$$< fakemessage, 1, fakemessage - 1, -, 19, 0 >$$

C. Fake Source 2 (FS2) Implementation

The FS2 protocol is similar to FS1. As described previously, the real source floods network messages to be delivered to the sink. FS1 and FS2 differ in the way that intermediate nodes communicate messages. In FS2 intermediate nodes forward each choose message to all of its neighbours. In FS2, when a node receives a choose message that has a hop-count value of 0, the node generates a random number R. If R is greater than a given threshold then the node becomes a fake source and begins generating messages. The message structures of choose and away messages are as in FS1.

The key difference between FS1 and FS2 techniques is that, in FS1 all intermediate and final nodes generate a random number to determine whether to forward a message or to become a fake source. On the other hand, in FS2 only the final nodes generate the random number to decide whether to become a fake source.

D. Design Decisions

By selecting a set of fake sources during operation, our protocol becomes adaptive, in the sense that for every real source, there exists a set of fake sources. This is in contrast with earlier work, where a set of fake sources in chosen at deployment time or is known *a priori* [5]. We are able to obtain fake sources which are a similar distance away from both the sink and real source by incrementing and decrementing the hop count.

V. Experimental Setup

In this section we outline the simulation environment and protocol configurations that were used to generate the results presented in this paper.

A. Simulation Environment

The simulation environment was based upon the JProwler simulator [4]. JProwler is a discrete event simulator that can accurately model sensor nodes and the communications between them. JProwler provides two radio models, Gaussian and Rayleigh, which determine the signal level of transmissions and the communication range of nodes. The Rayleigh model was selected for use in all experiments because it models the situation where sensor nodes have high mobility, which is consistent with the assumption that an attacker will have high mobility within a sensor network. An experiment constituted a single execution of the simulation environment using a specified protocol configuration, network size and safety period. An experiment terminated when the source node had been captured or the safety period had expired.

The JProwler simulator was extended to allow the safety period, capture ratio and total energy consumption to be monitored during simulation. Energy consumption was measured independently for each node in the network. The adopted energy model was consistent with [11], thus values for node voltage (V_{node}), current at idle (I_i), current at send (I_s) and current at receive (I_r) were required. As in [11], $V_{node} = 3V$, $I_i = I_r = 7mA$ and $I_s = 21.5mA$. All nodes were assumed to operate at maximum power, thus the transmission strength of each node was also maximal.

B. Network Configuration

A square grid network layout was used in all experiments. Experiments were performed for network sizes of 11, 15, 21 and 25, i.e., networks of 121, 225, 441 and 625 nodes respectively. A single source node generated messages and a single sink node collected messages. The source and sink nodes were distinct. Messages were generated at a constant rate of 1 message per second. The sets of experiments for each network size were performed for five source node locations; the four corners of the grid and a random location at the perimeter of the grid. To ensure the validity of the results presented, 100 repeats were performed for each source location. The sink node was located at the centre of the grid. Nodes were located 28 meters apart. The node separation distance was determined analytically, based upon the static fading values calculated by the adopted radio model. This separation distance ensured that messages (i) pass through multiple nodes from source to sink, (ii) can move only one hop at a time and (iii) can only be passed to horizontally or vertically adjacent nodes.

C. Protocol Configuration

All protocols were implemented according to the descriptions given in Section IV. The flooding protocol was used as a baseline against which other protocols were measured. All experiments involving FS1 and FS2 were run with threshold values of 0.5, 0.6, 0.7, 0.8 and 0.9.

D. Protocol Extension

Unique Messages (UM): In FS1 and FS2 fake sources generate fake messages which are identical to those generated by a real source. In networks with more than one fake source node this results in a recipient, i.e., an attacker or intermediate node, the dropping messages from two different fake source nodes on the basis that the messages were identical. If fake source nodes generated unique messages, duplicates would never be encountered and hence this message dropping could not occur. The unique messages extension is intended to ensure that an attacker will be forced to relocate more frequently. However, it should be remembered that the energy consumption of intermediate nodes is likely to increase due to increased network traffic.
Multiple Attackers (MA): The possibility of multiple attackers is explored by having four attackers co-ordinate their actions whenever a new message is received. The network grid is divided into quadrants, where each attacker was assigned a quadrant within which to operate. When an attacker receives a new message, they move to the sender of the message and instruct all other attackers to drop messages which are identical to the received message. The extension was run in conjunction with the unique messages extension, as it seeks to ensure that a received message provokes a response from exactly one attacker.
Increased Rates (IR): To this point it has been assumed that real sources and fake sources broadcast messages at a rate of 1 message per second. The increased rates extension observes protocol performance when the broadcast rates of fake sources is increased to 2 and 4 messages per second.

VI. Results

In this section we present the results generated by the described experiments. We first implement a distributed eavesdropper as a single mobile attacker. We then focus on another implementation of the multiple attacker variant of distributed eavesdropper, investigating the impact of this implementation on the fake source technique.

Table I: Safety period for network sizes under test

Network Size	Average Time Taken (secs)	Safety Period (secs)
11×11	16.00	32.01
15×15	23.41	46.83
21×21	34.74	69.50
25×25	42.89	85.77

A. Single Attacker on Flooding

The flooding protocol is used as a baseline routing technique, against which we will compare all privacy-aware routing protocols. The reason for using flooding as baseline is that (i) it has a high message delivery ratio, (ii) a subset of messages gets delivered along the shortest path from source to sink and (iii) it has been shown to offer poor levels of privacy.

A concept called safety period was introduced in [5] to capture the number of messages that has to be sent by the real source before it gets detected. In general, for maximum privacy, the safety period should ideally be high. In this paper we use an alternative, but similar, definition for safety period. For each network size, using flooding, we calculate the average time it takes to detect the real source / capture the asset. Then, when running simulations for privacy-aware protocols, we allow for a higher safety period, since the premise is that the proposed routing techniques will provide a higher source location privacy and may require more messages. The reason for this definition of safety period is that it bounds simulation time. The safety period, for each network size, for flooding is shown in Table I. Observe that the safety period is twice the average time taken for source detection / asset capture.

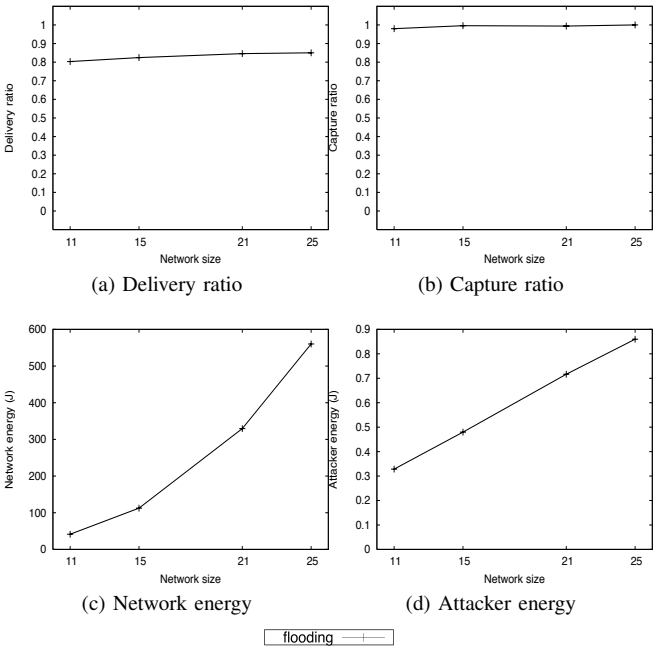
B. Single Attacker on FS1

The first phase of FS1 is a flooding phase, during which the real source floods the network with messages. Upon receiving the first of these messages, the sink sends a choose message to h nodes, where h is the distance between the source and sink. Thus, for a threshold value τ, $h+1$ nodes will decide to become a fake source based on Equation 1.

$$(1-\tau)^{h+1} \tag{1}$$

For example, with a threshold value of 0.9 and a distance of 5 from source to sink, the probability of a given node becoming a fake source node is 0.000001.

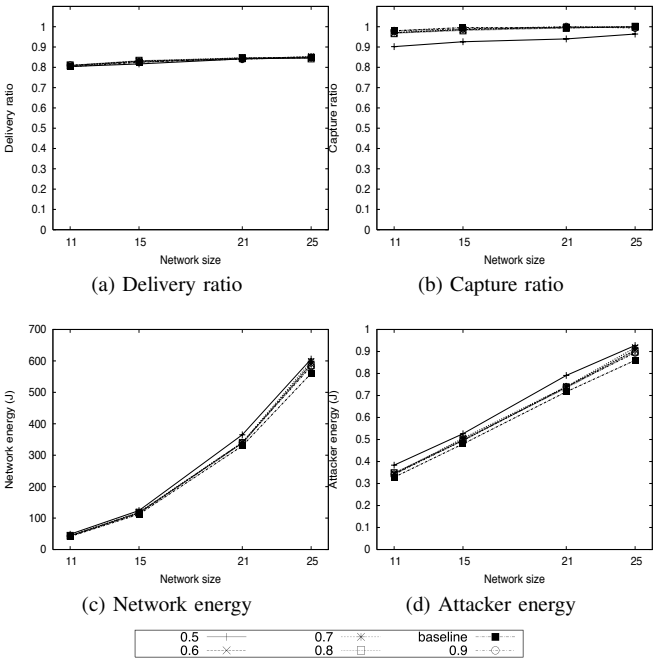
We observe from Figure 2b that FS1 offers a similar level of privacy as baseline routing, i.e., FS1 provides poor privacy as the capture ratios are comparable, especially when the threshold is high. This is due to the low number of fake sources selected, which is due to the very low probability of a node being selected as a fake source. This low number of fake sources is reflected in the network energy consumed.



(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 1: Flooding (baseline)



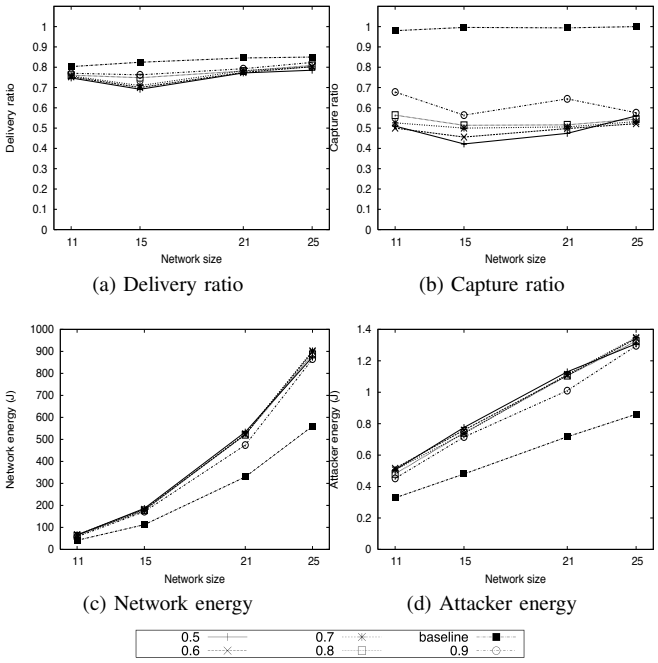
(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 2: FS1

C. Single Attacker on FS2

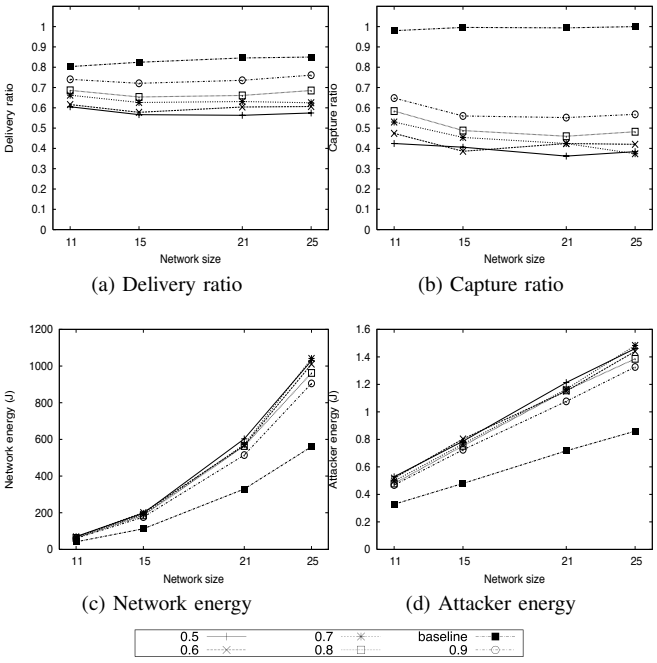
The first phase of FS2 is a flooding phase, during which the real source floods the network with messages. Upon receiving the first of these messages, the sink sends a choose message and each intermediate node becomes forwarders of



(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 3: FS2



(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 4: FS2 with UM

the message. Only potential fake sources generate a random number to decide whether to become a fake source.

We observe that this technique significantly improves upon the FS1 technique. To determine the level of privacy imparted by the FS2 technique, a closer look at the capture ratio from Figure 3b shows that the technique provides a significant improvement on privacy by reducing the capture ratio by as much as 50.5%. On the other hand, the delivery ratio is comparable to that of baseline routing (flooding) since the technique does not generate significantly more messages than in baseline routing, and thus not resulting in many message collisions. The network (resp. attacker) energy spent to provide privacy to (resp. capture) the asset increases, but are roughly commensurate.

D. Single Attacker on FS2 with UM

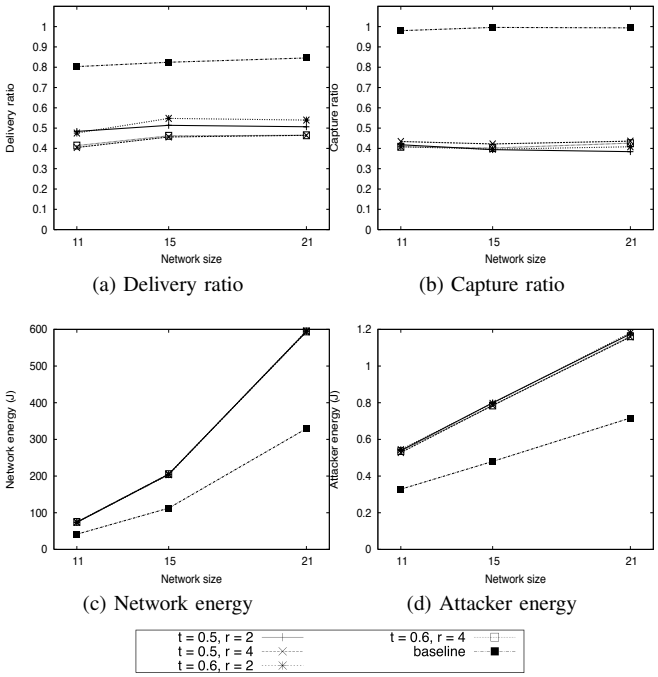
Combining FS2 and the UM extension involves every fake source broadcasting messages that are unique.The intention here is to promote more frequent attacker relocation.

Figure 4c shows how incorporating the unique message extension increases network energy consumption. This increase, which is attributable to the increased volume of traffic on the network, can be as high as 75.9% with respect to baseline routing, whilst the corresponding increased using only FS2 was 60.4%. Broadcasting unique messages has a negative impact on an attacker. The larger volume of network traffic means that an attacker receives more messages and consumes more power. As messages are unique, an attacker must also relocate more frequently and will take longer to find a real source. The consequences of this can be seen in Figure 4b, which shows that the capture ratio can be reduced by as a much as 60% compared to flooding. This level of privacy is also an improvement over FS2, which reduced the capture ratio by up to 50.5% compared to the same baseline.

E. Single Attacker on FS2 with UM and IR

We now observe the performance of the approach offering the highest levels of privacy, i.e. FS2 and UM, when message broadcast rates are increased to 2 and 4 messages per second.

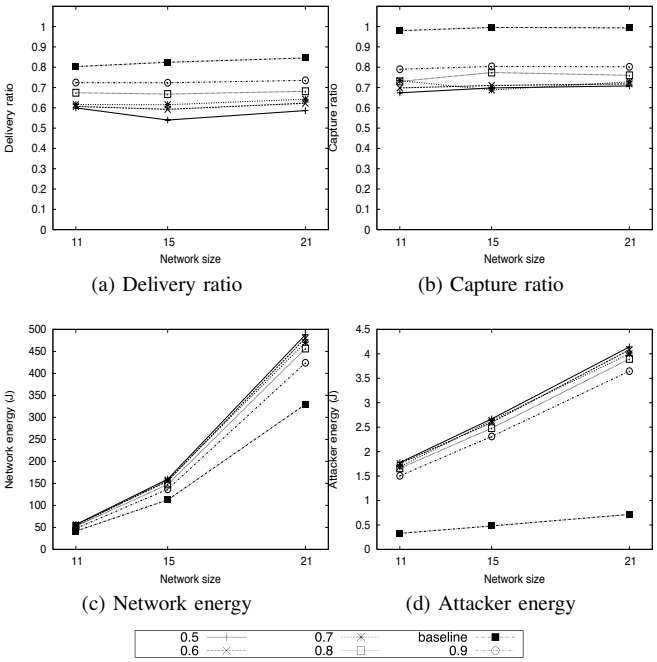
Figure 5c confirms the intuition that network energy increases with broadcast rate, i.e., broadcasting messages frequently increases energy consumption. It can be seen from Figure 5a that increasing the frequency with which messages are broadcast reduces the delivery ratio, though Figure 5b shows that the capture ratio remains stable at around 0.4. This is because nodes have to generate a random number to decide whether to become a fake source, thus in some situation no fake sources were generated, i.e., no potential fake source generated a random number greater than the threshold, meaning that an attacker can find the real source within the safety period. This is supported by the fact that proportion of simulations with zero fake sources was 30-40%. We conclude is that, whenever there are fake sources in the network, robust privacy is provided. Observe that the threshold parameter provides a tradeoff between the number of fake sources (hence network energy) and capture ratio (hence source location privacy). A lower threshold results in a lower capture ratio and higher energy consumption.



(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 5: FS2 with UM and IR



(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 6: Multiple attackers on FS2 with UM

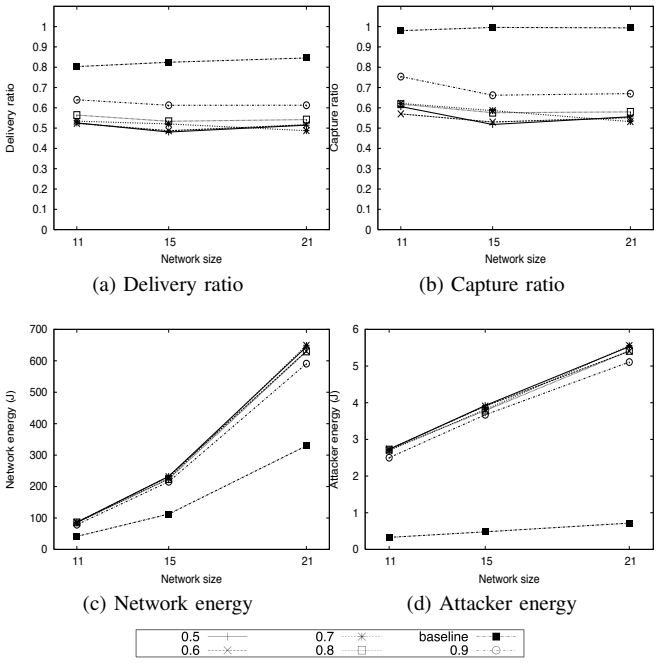
F. Multiple Attackers on FS2 with UM

To this point FS2 with UM has been shown to provide the best location privacy, achieving reductions in the capture ratio of up to 60% with reduced network energy. We now observe how this extended protocol performs in the context of multiple attackers, which is another possible implementation for distributed eavesdropper [3]. Here, attackers uses only *minimal inference* to coordinate, i.e., attackers coordinate only to ensure that no more than one attacker relocates in response to any single message.

Figure 6b shows a increase in the capture ratio of approximately 100% over FS2 and UM. This increase can be explained by the simple coordination between attackers. If an attacker has a fake source within its operating quadrant, it will receive corresponding fake messages and then prevent the other attackers from reacting to the associated fake source, even when they receive the same fake messages. One attacker, A, will have a quadrant that has the real source. As other attackers will receive fake messages before they are received by A, A can move towards the real source whilst dropping messages from fake sources. The energy consumption associated with each attacker is increased in the context of multiple, coordinating attackers. When operating in isolation, an attacker only needs to receive messages. However, in the presence of multiple attackers, additional message must be sent and received in order to facilitate cooperation. The consumed network energy, number of fake sources and the delivery ratio are broadly similar to those for FS2 with UM, thus implying that these metrics are invariant to the presence of multiple attackers. An important point to observe is that, though a single mobile attacker and multiple attackers are viable implementations of a distributed eavesdropper, the fact that they have such different impacts suggests the possible existence of other dimensions to an attacker model that are not captured by the taxonomy proposed by Benenson *et.al* [3].

G. Multiple Attackers on FS2 with UM and PR

Since multiple attackers induce an increase in the capture ratio when using FS2 with UM, a simple technique to circumvent the coordination logic of the attackers, which is based on the premise that only one attacker should follow any given fake message, must be developed. To achieve this we adapt the Phantom Routing (PR) protocol proposed in [5]. Phantom routing is a technique whereby a real source sends a message on a directed random walk of length τ. After τ hops, the node that has the message behaves as the real source of the message and proceeds to flood the network with messages. The idea here is that, since different nodes will initiate the flooding, the attacker will not receive successive messages, thus making it difficult to capture the source within the safety period. Results for the adapted Phantom Routing approach are presented in Figure 7, which shows for FS2 with UM and PR in presence of multiple attackers, the capture ratio falls to around 50%, which is an improvement on using only FS2 with UM.



(a) Delivery ratio (b) Capture ratio

(c) Network energy (d) Attacker energy

Figure 7: Multiple attackers on FS2 with UM and PR

VII. Conclusion

In this section we summarise the achievements of this paper and discuss future work relating to source location privacy.

A. Summary

In this paper we explored different implementations, configurations and extensions of the fake source technique for source location privacy. We have detailed implementations of the fake source technique which avoid a prohibitively expensive pre-configuration phase and the requirement that fake sources to be known *a priori*. In the development of the proposed implementations we have made no assumptions regarding the capabilities of sensor nodes, except that they are capable of sensing and relaying data. We have shown that, under the implementations considered, it is possible to achieve a reduction in capture ratio of up to 60%. We also explained that the 40% miss rate is due to the fact that no fake source may be selected on some occasions. We have further investigated the privacy provided by FS2 with unique messages in presence of multiple attackers. Our results show that multiple attackers cause a significant increase in capture ratio, which can be reduced through phantom routing.

B. Future Work

In future work we plan to undertake a greater exploration of variants and extensions to the described techniques. In particular, we intend to investigate how to provide enhanced levels of security whilst minimising the energy consumption of sensor nodes in the presence of multiple attackers

References

[1] S Armenia, G Morabito, and S Palazzo. Analysis of location privacy/energy efficiency tradeoffs in wireless sensor networks. In *Proceedings of th 6th International IFIP-TC6 Networking Conference on Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet*, pages 215–226, November 2007.

[2] I C Avramopoulos, H Kobayashi, R Wang, and A Krishnamurthy. Highly secure and efficient routing. In *Proceedings of the 23rd Conference on Computer Communications*, pages 197–208, March 2004.

[3] Z Benenson, P M Cholewinski, and F C Freiling. *Wireless Sensor Network Security*, volume 1, chapter Vulnerabilities and Attacks in Wireless Sensor Networks. IOS Press, April 2008.

[4] JProwler. http://w3.isis.vanderbilt.edu/projects/nest/jprowler/, 2010.

[5] U Kamat, Y Zhang, and C Ozturk. Enhancing source-location privacy in sensor network routing. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pages 599–608, November 2005.

[6] L Lamport, R Shostak, and M Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.

[7] S-W Lee, Y-H Park, J-H Son, S-W Seo, U Kang, H-K Moon, and M-S Lee. Source-location privacy in wireless sensor networks. *Korea Institute of Information Security and Cryptology Journal*, 17(2):125–137, April 2007.

[8] K Mehta, D Liu, and M Wright. Location privacy in sensor networks against a global eavesdropper. In *Proceedings of the IEEE International Conference on Network Protocols*, pages 314–323, October 2007.

[9] C Ozturk, Y Zhang, and W Trappe. Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 88–93, October 2004.

[10] A Perrig, J Stankovic, and D Wagner. Security in wireless sensor networks. *Communications of the ACM - Special Issue on Wireless Sensor Networks*, 47(6):53–57, June 2004.

[11] V Shnayder, M Hempstead, B Chen, G W Allen, and M Welsh. Simulating the power consumption of large scale sensor network applications. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pages 188–200, May 2004.

[12] Y Xi, L Schwiebert, and W Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In *Proceedings of the 20th International Parallel and Distributed Processing Symposium*, 2006.

[13] J Yao and G Wen. Preserving source-location privacy in energy-constrained wireless sensor networks. In *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*, pages 412–416, June 2008.