Bangash YA, Zeng LF, Feng D. MimiBS: Mimicking base-station to provide location privacy protection in wireless sensor networks. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 32(5): 991–1007 Sept. 2017. DOI 10.1007/s11390-017-1777-0

MimiBS: Mimicking Base-Station to Provide Location Privacy Protection in Wireless Sensor Networks

Yawar Abbas Bangash, Ling-Fang Zeng*, *Member*, *CCF*, *ACM*, *IEEE*, and Dan Feng, *Member*, *CCF*, *ACM*, *IEEE*

Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology, Wuhan 430074, China
School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

E-mail: {yawarabbas, lfzeng, dfeng}@hust.edu.cn

Received July 12, 2016; revised August 9, 2017.

Abstract In a wireless sensor network (WSN), sink node/base station (BS) gathers data from surrounding nodes and sends them to a remote server via a gateway. BS holds important data. Therefore, it is necessary to hide its location from an inside/outside attacker. Providing BS location anonymity against a local and global adversary, we propose a novel technique called MimiBS "Mimicking Base-Station". The key idea is the integration of aggregator nodes (ANs) with sensor nodes (SNs), while fine tuning TTL (time to live) value for fake packets, and setting some threshold value for real packet counter *rpctr*. MimiBS creates multiple traffic-hotspots (zones), which shifts the focus from BS to the newly created ANs hotspots. Multiple traffic-hotspots confuse the adversary while determining the real BS location information. We defend the BS location information anonymity against traffic analysis attack, and traffic tracing attack. MimiBS gives an illusion of having multiple BSs, and thus, if the attacker knows any about AN, he/she will be deceived between the real BS and ANs. MimiBS outperforms BLAST (base-station location anonymity and security technique), RW (random walk), and SP (shortest path), while conducting routing without fake packets, with fake packets, without energy consideration, and with energy consideration respectively.

Keywords base station, location privacy, wireless sensor network, balanced energy consumption, aggregator node

1 Introduction

Providing security solutions with resource constraint equipment, using the wireless media, is a big challenge. Wireless signals are all around a node. It is difficult to prevent signal propagation. However, due to the popularity of wireless sensor networks (WSNs) in applications such as military, monitoring and surveillance, animal rearing and agriculture, and atomic reactors[1-2], WSNs are better candidates to use. It is necessary to provide WSNs with the basic security mechanisms and protocols that can guarantee a minimal protection to the services and the information flow by both hardware and software[3]. At the hardware level, physical attacks like node capturing and stealing must be protected, and at the software level, all the cryptography parameters such as confidentiality, integrity, and availability (CIA) must be ensured[3]. However, the security of WSNs is not limited to provide merely CIA.

WSNs are defined as a large number of low-cost, small memories (kilobytes, and megabytes), self-organizing, unattended, low processing capable, and distributed embedded[4] small sensor nodes. They communicate through an open channel (air) to collect some data from the surrounding interest, process it, and report it to the sink for further actions. A comprehensive survey about WSNs can be found in [5].

In a WSN, nodes generate a tremendous amount of traffic in all directions. Aside from the information contained in the packets, the generated traffic itself is a " hidden value". In a mission-critical system such as

Regular Paper

This work was supported in part by the National Basic Research 973 Program of China under Grant No. 2011CB302301, the Fundamental Research Funds for the Central Universities of China under Grant No. HUST 2014QN009, the Natural Science Foundation of Hubei Province of China under Grant Nos. 2013CFB150 and 2015CFB192, and the Higher Education Commission (HEC) of Pakistan.

*Corresponding Author

military, the communication pattern (frequent, time-specific, and lack of communication) can reveal useful information about traffic behavior. An adversary can exploit such a pattern to know about the military secrets: planning, short-range communication, and command change. In such a case, the adversary ignores the contents. He/she only eavesdrops (secretly listening to other's conversations) the traffic volume. Diffie and Landu said "the heart of a communications intelligence organization, however, is not cryptanalysis but traffic analysis[6]".

In a military application, such as field monitoring and surveillance, a base station (BS) gathers the data from surrounding nodes and reports that data to a remote server via a gateway. Consequently, traffic volume near the BS becomes dense compared with other nodes. The BS has important data about network topology and sensor nodes. It also has mission-critical and sensitive information[7]. Therefore, BS location information must be protected. Location privacy needs more than confidentiality[8]. Confidentiality helps to encrypt a message. If an adversary captures a message, he/she will not be able to read it. However, confidentiality alone cannot help to guard against traffic analysis attack[9-10]. Therefore, it is important to guard BS location information against traffic analysis attack and traffic tracing attack.

Traffic analysis is the technique to deduce information from the monitored traffic volume. An attacker can analyze the traffic volume without being aware of the contents of data, and ultimately, he/she knows about the BS location. In most cases, the traffic analysis attack is used to attack BS or to exploit its location privacy. An attacker can use expensive radio transceivers to detect message flow[11]. Whenever he/she sees a huge amount of traffic density, he/she deduces the hotspot location as a BS.

In a packet tracing attack, an adversary traces an individual packet to know its reporting target. This attack is used for both the source and the destination node. The packet tracing attack is more difficult compared with the traffic analysis attack. In the traffic analysis attack, the attacker only monitors the traffic volume, while in the packet tracing attack, the attacker monitors the particular packet's movement and traces. Multiple hotspots are used to guard against the traffic monitoring attack, while multiple random paths can guard against the packet tracing attack. MimiBS provides location anonymity against these two kinds of attacks efficiently.

The rest of the paper is organized as follows. Basics of the WSN architecture are presented in Section 2. Related work on WSNs about BS location privacy is presented in Section 3. Section 4 is about our proposed algorithm MimiBS, "Mimicking Base-Station to provide location privacy protection in WSNs". Section 5 covers experimental and simulation results. Section 6 is about discussion, and Section 7 concludes the paper.

2 WSN Basics

Fig.1 shows the basics of a WSN node. It consists of a power, a sensor, an actuator, a mobilizer, a processor, and a transceiver unit. The generator/power source provides energy for the whole system (node). The power unit manages the required amount of energy to all sub-units. The sensing unit senses different events (movements, humidity, ambient light, etc.), and reports to a sink or BS. In some cases, we have an optional mobilizer and actuator. The mobilizer moves the sensor node physically from one place to another, while the actuator is accompanied with an imaging device (camera) to take pictures of the interested locations. The position finding system determines the node's exact coordinates, which helps to locate any sensor node in the deployed network. The storage/processing unit is responsible for the overall operations: data processing, resource management, and operating system (OS) execution. A reference architecture for WSN is shown in Fig.2.

An important unit of a sensor node is the transceiver. It can send and receive data/signals. In the sensor node, the transceiver unit consumes more energy compared with other units, because the packet transmission process includes signal amplification. To maximize the sensor node's battery life, it is advised that a transceiver unit should be designed properly to consume less energy when conducting communication.

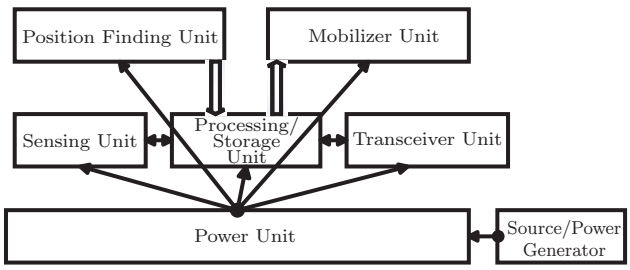


Fig.1. Basic diagram of a wireless sensor node.

As discussed in Section 1, MimiBS provides defense against traffic analysis and packet tracing attack. It is

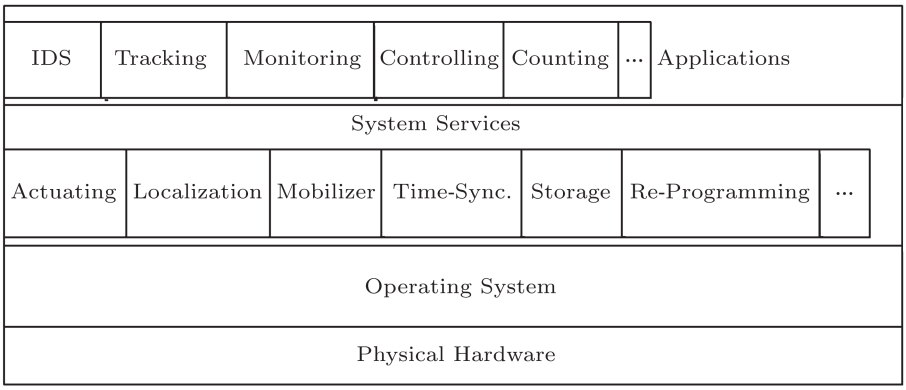


Fig.2. WSN reference architecture: the physical infrastructure includes sensor nodes (SNs), aggregator nodes (ANs), and a BS. The OS is responsible to manage the whole hardware. The application layer is used for tracking, monitoring, controlling, and counting.

worth explaining local and global traffic analysis. Local traffic analysis covers only a small portion of the total deployed area, and the related adversary is called a local adversary. Global traffic analysis covers the whole deployed area, and the related adversary is called a global adversary[12]. The local adversary can only monitor one position at a time. As he/she proceeds, he/she can monitor other places. While monitoring the second position, he/she is not able to monitor the preceding position any more. The global adversary has a global scope of the whole network. He/she can monitor any place at any time. Fig.3 helps to understand this concept. MimiBS conserves more energy, shifts traffic volume from BS to ANs, increases overall network life, and hides BS location information against traffic analysis and tracing attack.

Security is a complex process. Setting some parameter (TTL) may enhance one aspect (privacy), while it may degrade the other side (energy). A balanced trade-off among different parameters (energy, privacy, performance, and computations) in WSNs is desirable. However, designing a robust routing protocol, while addressing these parameters, is a complex task. Extensive prior work has been done to protect the BS location. Different techniques and methods have been proposed to provide some form of BS anonymity and location privacy. Some work focuses on energy consumption, some on routing algorithm, some on computational and delay performance, while some focuses on all of them. The overall goal of these methods is to hide the BS station in a better way compared with others. With the same intentions, we present MimiBS, where we show better privacy and anonymity for the BS, better energy consumption and minimum delay for nodes and packets delivery, and overall, easy management and flexibility due to the integration of ANs and SNs with fine-tuned TTL value.

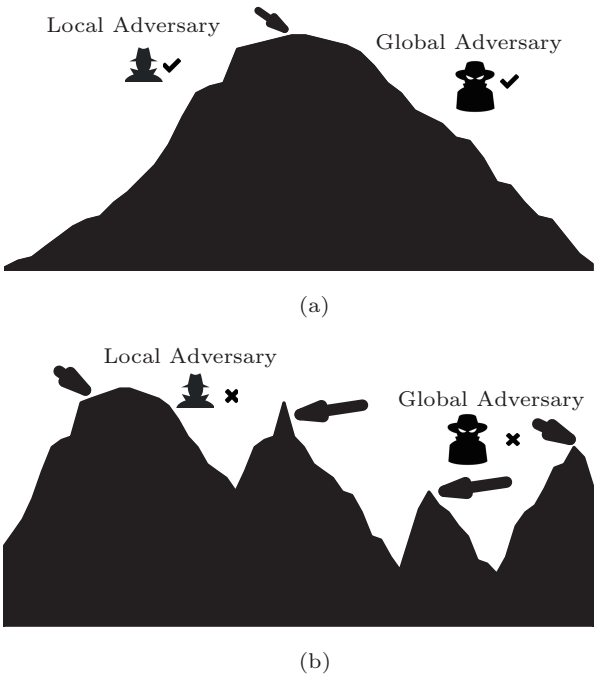


Fig.3. Local adversary vs global adversary. Because of a high traffic density (single BS), as shown in (a) single traffic density zone, both local and global adversaries can exploit BS location information. In (b) multiple traffic density zones, both local and global adversaries will observe multiple peaks, and, thus they will be confused to find the real BS location. MimiBS provides a novel technique to guard the BS location against traffic analysis and the traffic tracing attack.

3 Related Work

Wireless signals are invisible for a naked human eye. However, these are spread over all directions of the antenna. Because of this open-nature, it is hard to prevent an attacker from eavesdropping, and traffic analysis. To prevent the adversary from attacking the BS, the work

in [13] tries to increase randomness in traffic pattern, and combines it with fake paths to confuse the adversary when tracking a packet. Increased randomness with fake packets causes overhead, and extra energy consumption. This scheme, if powered with an insufficient amount of energy, encounters an un-availability issue at the end; for a prolonged time period, this scheme is not feasible.

The authors of [14] proposed random routing scheme (RRS) with dummy packet injection scheme (DPIS), which is further supported by anonymous communication scheme (ACS). RRS moves packets randomly to confuse the adversary, and does not give him/her a fixed path. For the traffic analysis attack, they proposed DPIS, which increases the dummy packets to hide the BS location. Randomness along with fake packets always comes with overhead such as packet collision and extra energy consumption. In [15], sink simulation and backbone flooding technique is used to deceive the adversary by creating virtual sinks, so that the communication between the real sink and the fake sink can be hidden from the attacker. But, the authors in [15] did not discuss any idea of ANs with fake packets injection, and at the same time, they did not discuss energy-based routing.

Concealing of the sink location (CSL)[16] uses dummy packets injection to defend against traffic analysis attack. The concept of deceptive packets to increase the anonymity of BS location is proposed in [17]. In [18], the authors proposed the protocol for sink location privacy via topology discovery protocol, and data transmission techniques. In all these techniques, the message overhead for dummy packets is increased. This overhead leads to shorten sensor network life, increases packet collision rate, increases packet drops rate, and ultimately, encounters network un-availability.

Base-station location anonymity and security technique (BLAST)[19] uses two types of nodes. Nodes near a BS are called BLAST nodes, while the others are called common nodes. BLAST nodes are different from sensor nodes, and they have a different range of communication. The data rate is controlled by injecting fake and dummy packets into the network. This scheme has a lot of overhead due to a large number of dummy packets. In BLAST, the BS resides within the BLAST ring, where communication is followed by the shortest path algorithm. BLAST saves some time and energy; however, this technique is vulnerable to attack. The main disadvantage is that it cannot hide the BS very efficiently. Having a BS location inside a BLAST ring raises a high security flag. The adversary only monitors the traffic inside the ring, which reduces the traffic monitoring attack-time. He/she will not search for the BS outside the BLAST ring. Ultimately, he/she has a narrow search space for the BS location. BLAST prefers lower energy consumption over strong privacy. If an algorithm exposes BS location information, no matter how strong and efficient it is, it should not be used in security demanded environment. It can be used for other purposes, but not for BS privacy and security.

The work done in [20] creates fake packets, fake sinks, and fake sources. Having multiple fake entities incurs substantial amount of packet overhead, maximum collisions, faster energy drainage, and longer packets delay. The study in [21] introduces two ways for sink location privacy: creating fake sink location, and generating an equal amount of packets by all nodes in all directions. The creation of fake sink location is vulnerable to attacks, because it does not change the constant position of BS. An equal number of packets generated by all nodes in all directions give strong privacy; however, this scheme consumes more energy and incurs extra overhead.

In location privacy routing (LPR) scheme[22], real packets are combined with fake packets injection. LPR can minimize the traffic direction from eavesdropping. Traditional single path (SP) walk quickly delivers packets to the BS. However, SP walk is extremely vulnerable to attacks; there is only one path for packets to move forward. LPR provides path diversity by combining dummy packets to minimize the information that an adversary can deduce from the overheard packets. In LPR, the adversary is limited to deduce the true BS location, but the main disadvantage is the overhead of fake packets that are injected into the network to hide the BS location information. Incoming and outgoing packet traffic is equally distributed in all directions, which causes a very dense overhead. For path diversity, LPR provides a randomized path, which is further supported by fake packets injection (augmented overhead). This path diversity confuses the adversary while tracking any packet. In LPR, packets are not always towards the receiver, and re-transmission is needed, which incurs extra delay and energy consumption. Another source location privacy method is presented in [23], where authors provided privacy through routing modification, and energy preservation via an ant colony optimization.

Onion routing[24], a general-purpose infrastructure for private communication over a public network, pro-

vides anonymous connections. It focuses on low-latency Internet-based systems, and is not designed particularly for WSNs. Due to its large-computational overhead, it is not feasible for WSNs. From WSNs perspective, onion routing demands high computational resources. It uses public key encryption extensively at each layer to protect the data inside an onion, and thus incurs a huge computational overhead and a high power consumption. MimiBS provides a novel approach to hide the BS, while preserving/conserving nodes' energy, as discussed in Section 4. Another important technique called differential enforced fractal propagation (DEFP)[13] uses multi-path routes and fake packets. In this technique, multiple random areas of high communication areas are created to deceive the adversary. The adversary will treat these created hotspots as true BS locations. The creations of high communication areas are supported by fake packets generation. This overhead introduces extra cost in terms of energy and computation; due to the randomness, packet collision rate and loss rate are very high in DEFP.

Phantom routing[25] uses probabilistic flooding[26-27]. This method uses more energy, while delivering packets to the BS. This scheme suffers from packets' delivery uncertainty (we are not sure whether packets will reach the BS or not). The uncertainty causes other issues such as increased delay, information loss, extra computation overhead, and useless resource utilization. SP or the single path routing algorithm always selects the shortest distance between a node and the BS. Thus, when an adversary hears huge traffic at some location, he/she is at a high success to attack the BS. SP always leads to the sink, and thus it cannot be used for security. Quick packet delivery and minimum energy consumption are the main advantages of SP. The main disadvantage is the single path forwarding behavior, which exploits the destination location information. If someone wants to use SP, it requires an extreme hardware level support[25]. SP takes short time to reach the BS, while random walk (RW) takes long time, but RW is more secure compared with SP. RW consumes a lot of energy and cannot be used as a stand-alone scheme (it lacks security features). The main advantage of RW is its randomness. Randomness protects packet tracing attack; longer delay, un-certainty, and more energy consumptions are inherited problems in the RW algorithm.

The work in [28] proposed adopting buffering technique at intermediate nodes. A packet is buffered at the intermediate nodes before being forwarded to next nodes. The adopting buffering technique suffers from buffered-delay and extra computational overhead. The authors of [29-33] presented the privacy for location-based services (LBS), which helps users to get their interested services while they are busy in their own life and routine. In computer networking paradigm, LBS helps end-users to find the nearest suitable service like banks, restaurants, hotels, and other useful information. In BS location privacy context, it is desired to hide the location-based information of users from any sort of privacy attacks like data leakage or user information leakage.

To protect the traffic monitoring attack, the rate privacy technique is presented in [34]. It proposed a general privacy protection scheme, but not specifically for the BS. The studies in [35-36] discussed the source location privacy, which is also studied by phantom routing. This scheme is different from BS location privacy. Context privacy, for users having smart-phones, is studied in [37-39]. The proposed strategies are purely related to mobile contextual privacy for smart-phones.

In a two-tiered sensor network, packets reach the sink or the storage node quickly. The work done emphasizes the data privacy, and data integrity is studied in [40]. However, the authors of [40] did not discuss BS location protection, and furthermore, their work assumed that the BS and the storage node are trustee entities. This unrealistic assumption is impossible in WSNs, where the deployed networks, in some cases, are exposed and open (having no physical or boundary security). The authors of [41] proposed energy efficient privacy preserving secure data aggregation (EPSDA) to provide an energy efficient and secure data aggregation scheme for WSNs. However, they did not discuss BS location privacy explicitly.

4 Mimicking Base-Station to Provide Location Privacy Protection (MimiBS)

MimiBS aims at providing privacy for the BS to hide the BS location, and deliver packets quickly and efficiently with minimum energy consumptions, while giving an equal probability to the adversary for all ANs to behave/look like the BS. We provide defense against a global and local adversary. The global adversary has the global view of the entire network, while the local adversary has the limited local view of the network. Confusing the local adversary is very easy, while countermeasuring against the global adversary needs special and efficient techniques. We assume one better cryp-

tography technique for content privacy[42], which will ensure all the CIA and other crypto basics. A state-of-the-art survey can be found at [43], where authors provided a deep insight about different calculation techniques (multi-precision multiplication and squaring) for cryptographic keys in WSNs. For strong BS privacy protection, we also assume an adversary (global) can monitor all the deployed network area (the worst-case analysis).

MimiBS mainly focuses on two types of attacks: packet tracing and traffic analysis. The packet tracing attack is studied in [25], and the traffic analysis attack is studied in [13]. These attacks are already discussed in Section 1. In MimiBS, the topology is generated via the flooding algorithm[44]. In MimiBS, all nodes have a neighbor nodes list, and hop-by-hop encrypted communication is practiced to exchange information like node status and node parameters. To create multiple traffic zones and shift the focus from the BS to other ANs, the deployed model and the implemented algorithm provide BS location privacy very efficiently compared with previous methods discussed in Section 3.

MimiBS uses the uniform distribution for node placements in the deployed area. For random distribution, we can use Halton sequence, which generates random nodes intelligently. For a small number of nodes, the Halton sequence generates a random grid, while for a big network, the Halton sequence generates a uniform grid. We use Java and Matlab random functions. However, MimiBS can also accommodate a pseudo random number generator (PRNG) method called Mersenne Twister method[45]. According to Wikipedia, this is the most widely used PRNG①.

Fig.4 is the deployment model for the proposed MimiBS algorithm. SNs detect new events and forward them to their respective neighbor ANs. An AN does two jobs here. First, it senses or detects new events and reports them to the BS. Second, it receives data from other SNs and forwards the data to neighbor ANs and then ultimately, forwards the data to the BS. The BS resides in the center as shown in Fig.4, collects all the detected data/events (from SNs and ANs), and reports the data/events to the outside world/users for further actions.

This is the BS that is responsible for topology generation, and taking on time action against any malfunctioning in the network[46]. In MimiBS, the integration of ANs reduces delay, increases network life, eases network management, and above all, hides the BS location from adversaries. For this, the underlined protocol and algorithm used for ANs, SNs, and BS must work in synchronization to achieve the BS location anonymity.

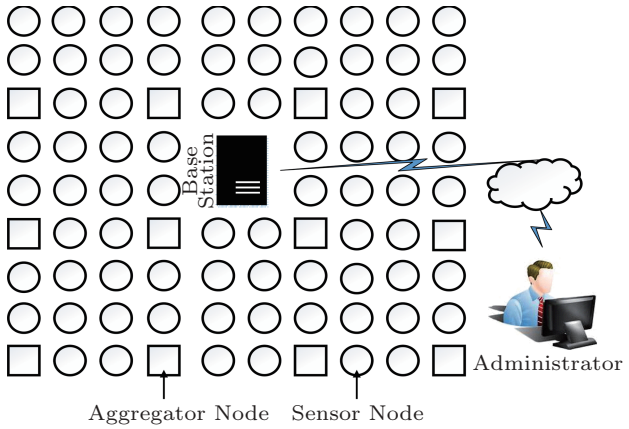


Fig.4. Block diagram of MimiBS.

Common life time of a WSN is 2∼3 months using two AA batteries with low duty cycle[13]. MimiBS can use the method in [47] for key management to protect hop-by-hop communication. MimiBS uses three types of nodes: SN, AN, and BS. SN has a small memory like mica2 whose transmission range is 55 m[48]. It has limited energy, range, and processing power. AN has a small memory, limited processing power, and more energy than SN, and its communication range (the area in which a node can send, and receive data/signals) is equal to three times of that of SN (if the communication range of an SN is 3 m, then the AN range will be 9 m). In our case, we can use mica2dot[48] for an AN, whose transmission power is higher than that of mica2. BS has greater power (energy), higher processing capabilities, and high memory capacity, and its range is the same with that of the AN. Note that the transmission power is the function of many factors like distance and surrounding environment[48].

MimiBS has two parts: energy-based algorithm, and without energy-based algorithm. Algorithm 1 considers both energy and privacy, while MimiBS without energy-based algorithm considers only energy (it preserves more energy, because it does not generate fake packets; however, it does not provide BS privacy). For the sake of content limitation, we do not mention MimiBS without energy-based algorithm (MimiBS without energy-based algorithm is not feasible for privacy protection). Node identification variable has three values:

①Stephen M. Machine Learning. CRC Press, 2011.

if it is 1, it will be an SN; if it is 2, it will be an AN; and if this value is 3, it will be a BS. A predefined value m related to distance is assigned to both the AN and the BS, while l is assigned to the SN. All nodes, except the BS, keep real-packet counter *rpctr* as a threshold value for fake packet generation. *rpctr* determines when to generate fake packets. Setting this value to 15, when any node sends 15 packets, fake packets will be generated with some *SomeOptimalValue*. By this way, MimiBS will not generate more fake packets (it preserves energy) in an equal direction contrary to [22].

Algorithm 1. Energy-Based MimiBS

```
1  Input: grid of size a × b, TTLF, rpctr, noOfMessages
2  Output: hopsCount, noOfSentMsgs, noOfRcvMsgs, remEnergy
3  Randomly pick a node, and set TTLF (TTL value for fake packet) = SomeOptimalValue, TTLR (Real Packet) = 0, rpctr (real packet counter) = 0.
4  /*Real packet generation*/
5  if NodeID = 1 & node distance = l then
6      /*We are at SN*/
7      TTLR = TTLR + 1, rpctr = rpctr + 1
8      Send the real packet to a neighbor AN node whose energy > the energy of all neighbor nodes of that node; if equal, select randomly.
9  end
10 else
11     if NodeID = 3 & node distance = m then
12         /*We are at BS*/
13         Get real packet with PacketID and TTLR + 1.
14     end
15     else
16         /*We are at AN now*/
17         TTLR = TTLR + 1, rpctr = rpctr + 1
18         AN forwards real packet to next AN whose energy level is the highest among all neighbor nodes, if equal, select randomly.
19     end
20 end
21 /*Fake packet generation*/
22 if rpctr = some-threshold-value then
23     Generate fake packet with TTLF = SomeOptimalValue, and forward the packet to the next node
24     while TTLF ! = 0 do
25         if NodeID = 1 then
26             For same energy, randomly select two or three neighbor nodes from neighbor nodes list; otherwise select two or three highest energy-level nodes and forward the packet to it.
27             TTLF = TTLF − 1
28         end
29         else
30             if NodeID = 2 then
31                 If the energy level is same, randomly select any neighbor node from neighbor nodes list; otherwise select the highest energy level node, and forward the packet to it.
32                 TTLF = TTLF − 1
33             end
34             else
35                 Discard the packet
36                 TTLF = 0
37             end
38         end
39     end
40     rpctr = 0
41 end
```

4.1 Packet Processing in MimiBS

Along with fine-tuned TTL values for fake packets, the *rpctr* also supports the hotspot generation to confuse the adversary. The higher the value of *rpctr*, the less the opportunity to generate fake packets, and vice versa, e.g., if *rpctr* is 20, the fake packets will be generated after 20 real packets, while if we set *rpctr* to 5, the fake packets will be generated after five real packets. When *rpctr* reaches some threshold value, e.g., 15, at this time both real packets and fake packets will be traversing in the network. The real packets will try to reach the BS, while at the same time, the TTL value for fake packets will be decreased at each next hop. This process will continue until the TTL value reaches zero. For example, if the real packets have already reached the BS, and the TTL value for fake packets is still not equal zero, this fake packet with some TTL value will be forwarded to other nodes until it reaches to zero. This process continues for all other real and fake packets.

After the network booting, there will be some real packets coming from surrounding nodes. To understand the packet processing in MimiBS, let us pick node 1, and this node receives packets from other nodes. At time $t1$, it receives one real packet; thus $rpctr = 1$, and at time $t2$, it receives another packet, so $rpctr = 2$, and so on until *rpctr* = *some-threshold-value* (in our proposed technique, the generation of fake packets depends on *some-threshold-value*; in this example, we assign 15 to *some-threshold-value*). At time $t15$, the value of this node reaches 15 (at this time, the *rpctr* equals *some-threshold-value*). As *rpctr* = 1 has already reached *some-threshold-value*, which is 15, at time $t16$, the TTL value for fake packets will be in action. At this stage, the generation of fake packets is started. We assign the TTL value to $SomeOptimalValue$, for example, $SomeOptimalValue = 5$. Now this fake packet with the TTL value 5 will be forwarded five times node after node until its value becomes zero. At time $t17$, a real packet may be received by some another node X, and at the same time, the fake packets will be received by

some other node, e.g., node $X + 1$. In all subsequent steps, this process continues.

4.2 Sensor Node

In MimiBS, every SN has at least one AN as a neighbor node. Initially, for real packets, when an SN detects an event, it sends the event to a neighbor AN with some TTL value to be incremented at the next hop. At specific time, when the *rpctr* value reaches some *threshold-value* (we set this value according to privacy requirements), the sensor nodes will generate and send fake packets to their neighbor nodes with the TTL value to be decremented at the next hop. This process hides the traffic tracing and analysis attack with some low energy cost. Low-end motes like mica2[48] can be used for sensor nodes as their processing power, and communication range is lower than high-end motes. The generation of fake packets is not constant. It is based on some random function or *some-threshold-value* of real packet count (*rpctr*). For example, the nodes will generate fake packets in a random direction if they have forwarded 10 or 15 real packets (energy preserving technique).

4.3 Aggregator Node

All ANs have two neighbor lists: ANs, and SNs. In the packet forwarding process, if the initial node is an AN, the forwarding process will be different from that of the SNs. An AN randomly selects another AN from its neighbor list (without considering energy factor), and forwards the packet to the selected AN with TTL value incremented by 1. At each next hop, we check whether the node is a BS or not. If it is a BS, we extract the data and do the desired action. If it is not a BS, the forwarding process repeats. Considering the energy factor, MimiBS does not randomly select the next AN. It selects another AN based on the remaining energy level of that AN, and checks again for the BS.

The generation of fake packets in ANs is different from that in SNs. Here, MimiBS does not send fake packets to all ANs' neighbor nodes, but only to a randomly selected node. This method does not incur huge fake traffic; it efficiently hides the BS, and prolongs the network life. High-end motes like mica2dot[48] can be used as ANs as their communication range and processing power is higher compared with low-end motes.

In a uniform distribution, every SN must have at least one neighbor AN. In practical situation such as dropping nodes from helicopters (for the deployment in a hostile environment, e.g., battle field), some SNs may fail to forward the data/events to some ANs (because some ANs are out of the communication range of some SNs). To guard against this phenomenon, we can drop more ANs to ensure the availability. In security applications, e.g., military, deploying redundant ANs can increase the total expenditure; however, the quantity of ANs is directly proportional to privacy. Deploying a large number of ANs yields strong BS' privacy and vice versa. A large number of ANs do not incur network complexity (all ANs have only a limited number of neighbor ANs). They even provide better packets delivery and BS anonymity.

4.4 Base Station

The processing power and memory capability of the BS is higher than that of the SN and AN. Initially, we randomly select a node from the grid to forward a real packet to its neighbors, and ultimately to the BS. In MimiBS, most of the traffic travels through ANs, but not through SNs. We use SNs to provide support for BS location anonymity.

BS can change the topology at any time. BS can also reset the whole network by sending some special packet (reset packet). Receiving this packet, the whole network will behave like a new-born network. This flexibility is good for more security reasons when we want to reset the network after some specific period of time (hours, days, or weeks).

With the collaboration of SNs and ANs, detected events are forwarded to a neighbor AN. The AN further, forwards packets to the BS with the real packet threshold count and fine-tuned fake packet TTL value. The integration of ANs with fine-tuned fake packet TTL value shifts the focus from the BS to other nodes, which generates more traffic peaks. Our proposed model in the mentioned way achieves BS privacy intelligently. Communication is encrypted in the algorithm.

4.5 Role of TTL

The role of TTL for real and fake packets is of special importance. TTL value for fake packets is the fine-tuned element of MimiBS. Both can affect the system's performance, and energy consumption. Choosing high-value TTL for fake packets generates huge traffic density; however, it hides the BS more securely. On the other hand, low-value TTL incurs low overhead in terms of energy; a small TTL value may exploit BS location information. There is a trade-off between privacy and energy using high-value TTL. The TTL

value for the real packets is incremented at each hop next until the packets reach the BS. This value (TTL) gives the delay performance. A high-value TTL (a real packet) shows huge delay, while a small value shows quick packet delivery (minimum delay). TTL values for fake packets are decremented at each hop next so that it can guard against traffic analysis and tracing attack; through this process, MimiBS generates automatic fake hotspots from ANs.

4.6 Packet Characteristics

There are four types of packets used in MimiBS: hello packets, real packets, fake packets, and reset packets. Hello packets are used in the start of the network building via flooding algorithm[44], real packets are used to carry user-data, and fake packets are used to confuse the adversary. Reset packets are used to reset the whole network. All packets have some fields, e.g., packet ID, packet type, and TTL value to carry out different operations.

4.7 Power of the Adversary

The adversary can use antennas and spectrum analyzers. He/she can also use the signal properties like the strength of the signal, and the angle of arrival for measuring the overhearing of packets. For traffic analysis, he/she sits in one place and monitors the traffic rate. If the rate is high, he/she deduces the BS location on high-traffic assumption. For packet tracing attack, the adversary follows one particular packet. All these techniques are for local adversaries. Global adversaries[49] have the global view of the overall network. We already discuss global and local adversary in Section 2.

MimiBS efficiently achieves good defense against global adversaries as well. We give a challenge to both adversaries to find the BS location. The higher probability the values, the lower the BS location anonymity, and the lower probability the values, the higher the BS location anonymity (if the value is near to 1, the BS location will be extremely vulnerable, and if it is near to zero, the BS location will be highly secured). Our simulations show that global adversary has a number of traffic peaks (for n peaks, the global adversary will have the probability of $1/n$). Based on his/her traffic analysis, he/she has an equal probability over the traffic peaks. Consequently, he/she will not be able to deduce the BS location.

4.8 Shifting the Focus from BS to ANs

MimiBS shifts the focus from the BS to the ANs. It is a novel method to provide BS location privacy. It gives adversaries an illusion that there are multiple BSs. Without ANs, shifting the focus from the BS is impossible (in our scheme); ANs successfully shift the focus from the BS towards other ANs. Multi-hops data transferring-technique gradually converges to one specific area. This area is closed to the BS. This is the place where the communication behavior of nodes is denser, and thus riskier. By analyzing this area, an adversary easily infers the BS location. The dense communication zone, which can exploit the BS location, is an inherited problem in all WSNs. MimiBS provides multiple communication zones to deceive the adversary.

In a sensor network, according to the Paretoś principle[50], 20% of the network nodes carry about 80% of the entire network traffic, and 80% of the network nodes carry about 20% of the entire network traffic. This means nodes near the BS, the 20% of all nodes, can carry about 80% of the entire network traffic, and the remaining 80% of network nodes can carry about 20% of the entire network traffic. This phenomenon creates a hot traffic pattern, which is extremely vulnerable to the BS attack. MimiBS shifts this pattern from the BS to other nodes. The Paretoś principle can be observed in many fields such as, finance, marketing, medical industry. For example, 80% customers do 20% shopping, while the remaining 20% customers do 80% shopping.

Proof. To support our model, we suppose a large area of radius R; sensor nodes are uniformly distributed with some number N, and R is large enough to hold nodes as many as possible. In this model, each node generates a message or a packet towards upper nodes until it reaches the BS. Assuming uniform distribution of nodes, this problem can be modeled as an area of a cumulative integral model as shown in Fig.5.

The area of the inside circle $A1$ is calculated in (1).

$$A1 = f(r) = \pi r^2. \tag{1}$$

To calculate the network traffic at $A1$, the integral of this area, i.e., the traffic at this area, is shown in (2).

$$Traffic_{A1} = \int_0^r f(r)\mathrm{d}r = \frac{\pi r^3}{3} + Constant, \tag{2}$$

where $f(r) = \pi r^2$, and $Constant$ refers to an integer.

The annular region area $R - r$ can be calculated as shown in (3).

$$\delta r = \pi R^2 - \pi r^2. \tag{3}$$

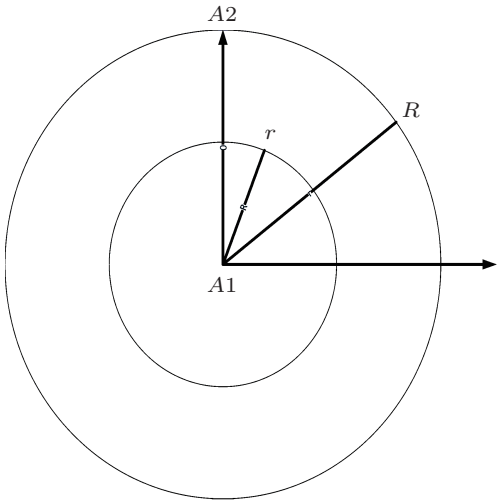


Fig.5. Integral model of a WSN traffic.

The total network traffic in the network can be calculated as shown in (4).

$$\begin{aligned} & Traffic_{A2} \\ &= \int_0^R f(r)\mathrm{d}r \\ &= \int_0^r f(r)\mathrm{d}r + \int_r^R f(\delta r)\mathrm{d}r \\ &= \frac{2\pi r^3 + 2\pi R^3 - 3\pi R^2 r}{3} + Constant. \end{aligned} \tag{4}$$

To prove our claim, we calculate the ration of whole network traffic to the small circle area $A1$, i.e., $\frac{Traffic_{A2}}{Traffic_{A1}}$. The calculation is shown in (5).

$$\frac{2r^3 + 2R^3 - 3R^2 r}{r^3} + Constant. \tag{5}$$

Putting different values for r and R in (5), the formula supports our claim (nodes near the BS, which are 20% of all nodes, can carry about 80% of the entire network traffic, and the remaining 80% of the network nodes can carry about 20% of the entire network traffic). When $r = 2.8$ and $R = 5$, the first part of (5) shows 3.822:1 (the network traffic inside 20% area is 79.26%, and the network traffic inside 80% area is 20.74%). When $r = 5$ and $R = 9$, (5) shows 3.944:1 (20% area carries 79.773% network traffic, and 80% area carries 20.226% network traffic). When $r = 9$ and $R = 16$, (5) shows 3.76:1 (20% area carries 78.992% network traffic, and 80% area carries 21.008% network traffic).

All these different values depend on the real 20% integral values. The value of r and R must be set according to the real network deployed area; otherwise unintelligently random values can generate some other results. It is not always the case to have 80:20; however, MimiBS is almost closed to this ratio. Constant value in (5) can help to set the Paretoś principle more smoothly. □

Definition 1. *In a sensor network,* 20% *nodes near the BS carry* 80% *of the network traffic of the conventional zone, while the remaining* 20% *of the network traffic is carried out by* 80% *of other zones. Since the sensor nodes in the network are uniformly distributed, the* 80% *of the coverage area occupies merely* 20% *of the whole network traffic. In* 20% *of area, the traffic is* 80% *of the entire traffic. Obviously, for a smart and expert adversary, the conventional zone is of special importance to carry out packet tracing and analysis. Thus, with such a knowledge, the adversary only chooses* 20% *of the network or the conventional zone as shown in Fig.*6. *In addition, conventional zone provides a small search area, and it gives minimum search time to find the BS location.*

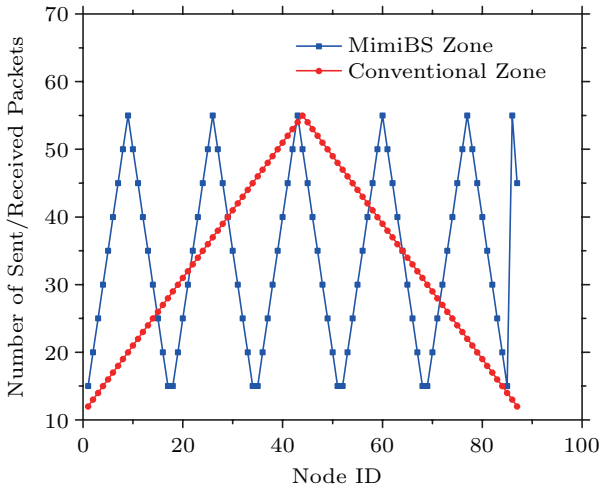


Fig.6. Conventional zone vs MimiBS zone.

Definition 2. *In a sensor network, the communication cycle with the highest traffic density is the hot spot of the particular sensor network. We call this spot MimiBS zone. This is the focal point of a WSN network to be defended. If the AN is not used, the aggregation behavior of data only falls into one place (the conventional zone). Traffic density is at the highest peak near the BS. If the attacker has a global vision, he/she can find the BS location through traffic monitoring attacks. In MimiBS, we shift this focus from conventional to MimiBS zones.*

As shown in Fig.6, MimiBS can deceive the adversary by having multiple traffic density zones (MimiBS

zones); these zones are automatically created by ANs' traffic. All the highest traffic density zones created by ANs can be seen as hot spots by the adversary. In this way, the traffic is never ever converged to one place. Additionally, MimiBS makes BS' search difficult for the adversary, and keeps him/her busy in MimiBS zones. MimiBS spreads the BS location over a large space. To attack the BS station, the adversary will encounter maximum computational overhead, labor cost, and a long-time span.

5 Performance Analysis and Simulation Results

5.1 Evaluation Methodology

MimiBS is very flexible. It depends on the environment where we use it. If we need maximum privacy and prolonged network life, we can change some parameters (TTL value) in Algorithm 1 to work for that particular purpose. Energy-based part of MimiBS is well suited for the BS protection, because it saves energy and provides the anonymity.

In the intelligent behavior of energy consumption, MimiBS conserves energy and delivers packets quickly, while hiding the BS. All nodes (SNs and ANs) select the next neighbour node based on its maximum energy level. Neighbor nodes have the latest update of the energy level of the neighbor nodes of each AN. MimiBS selects only the node whose energy level is the highest among all neighbor nodes. To preserve nodes' energy, the energy update packet is shared among nodes at some proper interval of time. This technique leads to a novel randomness, which we call the intelligent randomness.

When a node sends or receives a packet, its energy capacity is decreased, and its energy level is updated. Then, when the same node sends or receives a packet, its energy capacity is checked and compared with other nodes. Definitely, at this time, its energy capacity will be lower than or equal to that of other nodes. In the case of a low energy level, this node will not be selected at the instance. In MimiBS, equal energy level for all neighbor nodes is very rare. At least, there is one node whose energy will be less than the respective neighbor nodes of each AN. This intelligent mechanism introduces a pattern, which we call the intelligent randomness, whose biggest advantage is the balanced energy distribution (all nodes will drain together; it will not be the case that one node will have a high energy level, while another will have zero energy level).

MimiBS incorporates different energy levels according to the nodes' remaining energy capacity. If the energy levels of neighbor nodes are same, they will be selected randomly. If the energy level of a node is greater than 85%, it will be regarded as a high-level $L1$. If it is more than 60%, it will be regarded as a good-level $L2$. If it is greater than 45%, it will be regarded as an average level $L3$. If it is more than 30%, it will be regarded as a low-level $L4$. If it is less than 30%, it will be treated as a flag-level $L5$. All nodes fall into one of these five levels, and Algorithm 1 selects the highest energy level as it is desired for better energy consumption and BS location anonymity. For example, if the AN has an energy level of 84%, it will fall into level $L2$, and the node field will show its energy as level $L2$. This energy level is shared among its neighbor nodes. While forwarding packets to the next neighbor node, the source node first selects the node whose energy level is higher than the other neighbor nodes, and the process continues until battery power drains completely.

5.2 Experiment for Hops Count

The hops count parameter gives the latency information. The larger the hops count value, the larger the delay (packets take long time to reach the BS), and vice versa. When we increase the number of packets to 1 000, for 20 ANs, the average hops count value was 7.45 (a packet reaches the BS through eight sensor nodes approximately). This implies that the ANs concept can effectively deliver packets with minimum hops count to the BS.

Fig.7 clearly shows that, in MimiBS, the hops count (delay) is in between that of random walk (RW) and shortest path (SP). Here, we have not included the traffic of sensor nodes, because the maximum traffic is carried out by ANs. In the packet forwarding process, a maximum number of packets are exchanged among ANs, and not among SNs.

In Fig.8, the area near ANs is highly activated as compared with a non-aggregated area. This diagram is based on Algorithm 1, while it ignores the energy parameter. However, it still provides some location anonymity (because of the MimiBS internal mechanism, the adversary will see four peaks). *RP* represents the real packet, while *FP* represents the fake packets. When packets are received in MimiBS without generating fake packets, the comparison result is shown in Fig.9. The BS (node 13) has received maximum packets; the adversary can attack the conventional zone easily.

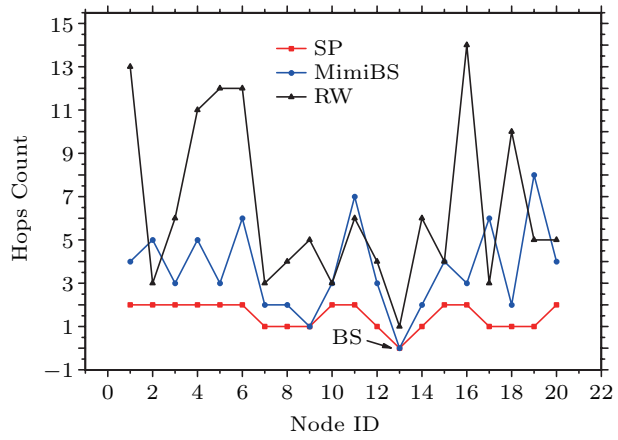


Fig.7. Hops count.

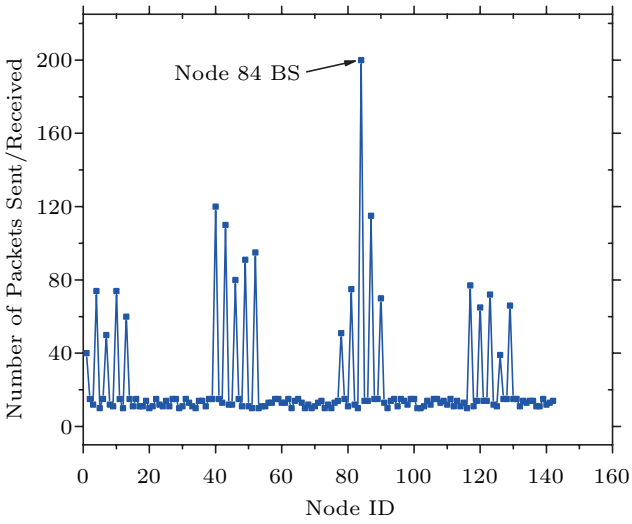


Fig.8. Packets processing with modified RW-MimiBS.

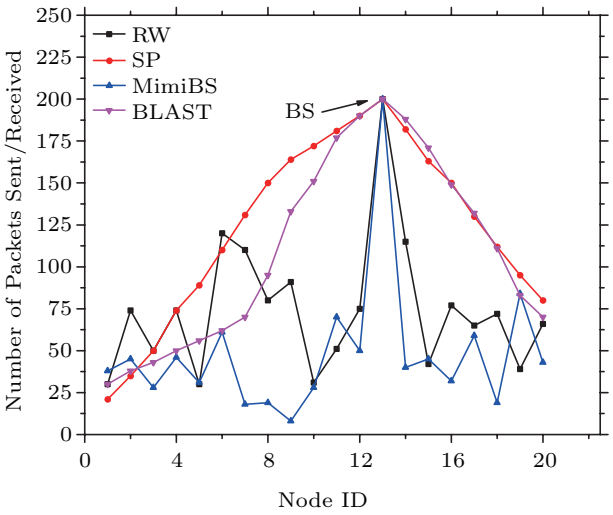


Fig.9. Different comparisons show MimiBS outperforms the other methods while hiding the BS.

Fig.9 shows protecting the BS location without generating fake packets. The BS is vulnerable to attacks. In addition, there is no other node to behave like the BS to deceive the adversary (because of the single traffic peak, the adversary monitors the traffic, and deduces the high communication area as a BS location).

In Fig.9, while delivering a packet to the BS, SP is much quicker than RW. Note that, in all these methods (SP, RW), MimiBS method is also embedded (modified SP and modified RW). None of these methods hides the BS location; however, MimiBS performs better than the others. To hide BS, MimiBS augments fake packets with real packets as shown in Fig.10. MimiBS tries to smooth the graph so that all ANs areas look like BS. Fig.10 demonstrates the traffic behavior with fake packets, which increases traffic density. This provides better BS anonymity compared with non-fake packets algorithm.

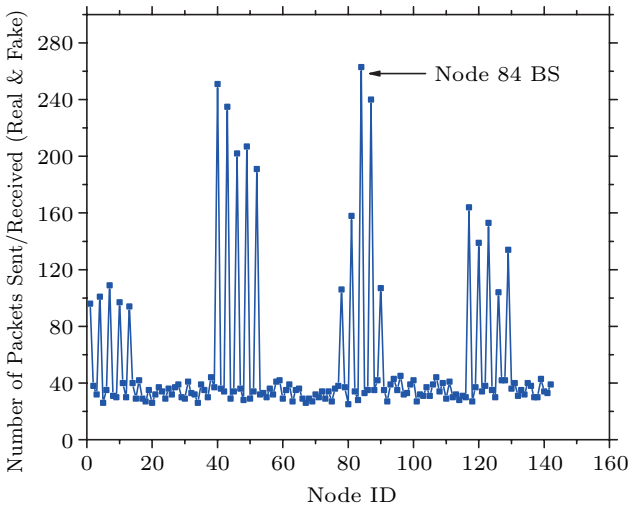


Fig.10. Packets received along with fake packets.

In Fig.10, there are only four peak regions, where the BS location is hidden. In such a small peak region, it is easy for the global adversary to attack/destroy all peaks (he/she will still not be sure about the real BS location). To provide strong privacy, it is advised to deploy more ANs in a large area. This point is already discussed in Subsection 4.3. A large area with hundreds of ANs provides high BS privacy. For example, for n peaks, the global adversary will have the probability of $1/n$.

TTL value is of great importance in MimiBS. Increasing TTL value will yield a dense traffic and more energy consumption; however, it provides strong BS anonymity. It is the choice of application to set the

TTL parameter. High-value TTL means heavy traffic, high energy, and strong privacy; low-value TTL means minimum privacy, little energy consumption, and low traffic density.

5.3 Experiment for Energy Consumption

For the initial step, the average hops count is bigger, because the network is merely started up, and there is no battery drain for a node. Algorithm behavior looks like a true random. After some operations (like packet transmission), Algorithm 1 converges to its best performance.

To prevent the conventional zone's attack as shown in Fig.9, Fig.11 shows the intelligent behavior of the energy-based algorithm. Because of the ANs, no single node will be in maximum or minimum energy level. MimiBS efficiently achieves better energy distribution. We call this distribution as the balanced behavior energy consumption. Achieving balanced behavior energy consumption demands a great deal of underlined protocol, deployed network model, and physical layout. This behavior prolongs the network life and provides longer availability over the course of entire network life.

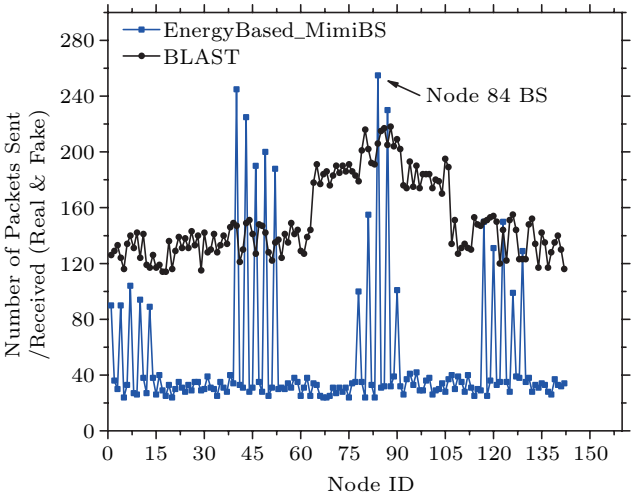


Fig.11. Energy-based traffic behavior.

First-order radio formula[51], where authors discussed to estimate the energy needed to send a packet of a bits of data from a transmitter to a receiver, can be used to model the energy consumption in WSNs. Transmitting packets consume more energy compared with receiving packets. In a transmission, signal amplification is an extra energy consumption parameter along with transmitting electronics. In a packet receiving process, only receiving electronics is the energy consumption parameter.

The general formula for transmitting a bits is shown in (6), where $E_{Tx}(a)$ is the energy that the radio circuit needs to consume in order to process a bits, aE_{Tx} is the amount of energy consumed by processing a single bit by the radio circuitry, and $E_{\text{amp}}(a,b)$ is the energy needed by the radio amplifier circuit to send a bits of the message over distance b. For receiving a bits, the receiving formula is shown in (7), where aE_{Rx} is the energy consumed by receiving circuitry for processing a single bit.

$$\begin{aligned} E_{\text{totalTx}}(a,b) &= E_{Tx}(a) + E_{\text{amp}}(a,b) \\ &= aE_{Tx} + E_{\text{amp}}(a,b). \qquad (6) \\ E_{totalRx}(a) &= E_{Rx}(a) = aE_{Rx}. \qquad (7) \end{aligned}$$

In Fig.11, when Algorithm 1 generates fake packets, the BS is almost hidden within the ANs. An attacker cannot attack the BS due to traffic analysis. Increasing ANs' quantity provides strong privacy for the BS location. BLAST has only one hotspot (the real BS, BLAST nodes inside the ring are not dynamically created), and it does not generate fake hotspots randomly as generated in MimiBS. Therefore, it cannot guarantee BS privacy (the BS location inside the ring raises a high security flag for the global adversary). Additionally, BLAST uses randomness outside the BLAST ring, which utilizes more energy as compared with MimiBS. The delay outside the BLAST ring is very high as compared with that inside the ring. For the simulation results for a small number of ANs, MimiBS generates four hotspots. The number of multiple traffic peaks or hotspots is directly proportional to the number of ANs. If we increase the number of ANs and SNs, we will have more hotspots. This will give a strong challenge to the adversary to find out the real BS.

5.4 Remaining Energy Comparison

In the delay[52] model, MimiBS uses a simplified point-to-point delay for packet delay analysis. To find the complete delay for a single packet, processing delay can be treated as a constant time Tp. The queuing delay can be considered for continuous data sampling applications in WSNs. Total delay can be calculated by adding processing delay, queuing delay, and propagation delay. (8) is the general formula to model point-to-point delay. T_p is the processing delay, $Delay_{\text{que}}$ is the queuing delay, and $Delay_{\text{prop}}$ is the propagation delay. We simulate the case related to the number of packets received or transmitted by any node. Initially,

we assign a constant number such as 300 Joules of energy for SN, 900 for AN, and 1 500 for BS. When a node receives or sends a packet, the energy is decreased by another constant such as 1 Joule. This simulation is shown in Fig.12.

$$Delay_{\text{total}} = T_p + Delay_{\text{que}} + Delay_{\text{prop}}. \quad (8)$$

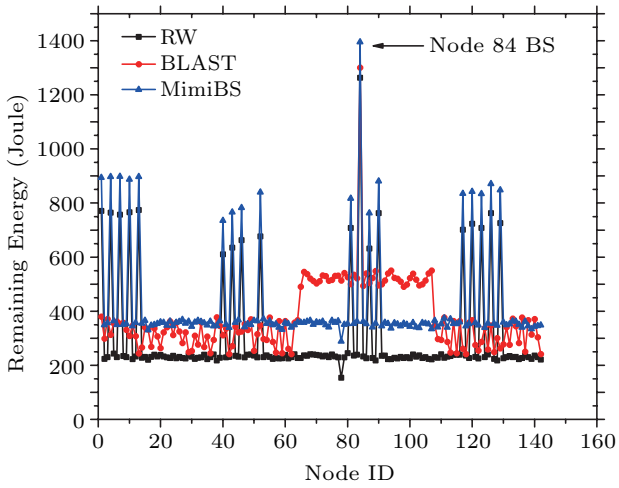


Fig.12. Remaining energy comparison.

A network with more sensor nodes is much secure as compared with that with a small number of nodes. To achieve maximum privacy, it is advised to deploy more ANs; in other words, MimiBS provides strong protection for big networks as compared with small networks.

MimiBS energy consumption is better as compared with the other schemes. MimiBS provides balanced energy distribution along with prolonged network life. Battery (energy) drain is not random in MimiBS, which achieves strong availability. BLAST consumes more energy as compared with MimiBS, because BLAST uses randomness outside the ring, which increases delay and consumes energy.

Table 1 shows the advantages of MimiBS. It provides balanced energy consumption, which is the most important factor of modern WSN era. The random selection suffers from unpredictable network life, while the energy-based routing in MimiBS provides minimum delay, and prolonged network life. The shortcoming of MimiBS is a bit more processing compared with SP or RW; however, SP and RW are not used to provide BS privacy.

6 Discussion

MimiBS protects BS location anonymity via fine-tuned TTL value for fake packets, *rpctr* (real packet counter or threshold), and ANs' integration. The intelligent randomness is provided by the TTL value and *rpctr* (which provides multiple paths to a void tracing attack). ANs' integration provides multiple traffic peaks to shift the single traffic focus from the BS over other ANs. (Nodes near the BS, which are 20% of the network nodes, carry about 80% of the entire network traffic. MimiBS shifts/spreads the 80% of network traffic over the remaining 20% of network nodes.) We have applied different anonymity metrics such as *rpctr*, and the TTL value for fake packets to protect BS privacy. Our experiments show that global adversary has the attack probability of $1/NO_{\text{Peaks}}$. According to simulations, and average results, MimiBS strongly protects the BS location against the global and the local adversary. It delivers packets quickly, and conserves energy.

In all our simulations, we have shown only four peaks, because our experiment uses 149 nodes (19 ANs, 1 BS, and the remaining are SNs). When we increase

Table 1. Analysis and Comparison of Different Parameters in WSN

Method	Energy Consumption	Delay	Security	Traffic Tracing	Traffic Monitoring	Network Life
SP	Low	Minimum	At high risk	At high risk	At high risk	Long
RW	High	High	Good compared with SP	Good	At high risk	Short
RW with fake packets	Very high	Very high	Good	Very good	Good	Less than RW
MimiBS	Balanced	Initially high, but after some time, will behave like SP	High value TTL, high security, low value TTL, low security	Very strong	Very strong	Balanced
BLAST	Higher than MimiBS	Overall high	BS limitedly-secured inside ring	Strong	Strong	Good
LPR	High	High	Very good	Strong	Very strong	Good

the number of nodes, the number of peaks increases accordingly. The number of peaks is directly proportional to the number of nodes. Therefore, in a large area, we will have definitely more nodes, and consequently, we will have more peaks. More peaks provide strong privacy. For example, in the case of 10 peaks, the adversary's probability will be 1/10, while in the case of 100 peaks, the adversary's probability will be 1/100. In addition, the global adversary can monitor the whole deployed area; if the deployed area is small and the network has a small number of ANs, BS location privacy will be at risk (even still, the global adversary will not have the success probability of 1). Therefore, it is advised to deploy more ANs to provide strong BS location anonymity. There is a trade-off among strong privacy, ANs' quantity, and deployed area. MimiBS provides strong protection for a big network compared with a small network.

Even for a small number of peaks, the adversary will not be confident about the real BS location. He/she will be confused among different peaks (small or high). Based on his/her traffic analysis attacks, he/she cannot find out the BS location. If he/she wants to destroy the real BS, he/she has to destroy all peaks, which is an inefficient way (in terms of efficiency, this is a wastage of resources utilization).

TTL values for fake packets can tune the network traffic. An optimal fine-tuned TTL value governs the generation of fake packets. We have performed different experiments to obtain an optimal value (that could balance privacy and energy consumption) for TTL (fake packets). However, the optimal TTL value depends on the environment and applications for which the network is deployed (because of the WSN traffic nature, it is difficult to predict this value in advance). For high privacy, a high TTL value is recommended and vice versa. In MimiBS, setting an optimal TTL (for fake packets) is important. A high value generates more traffic surrounding the ANs than traffic surrounding the BS. In this case, the traffic density that surrounds all ANs will be much higher than the BS; however, this will drain battery quickly. For the sake of equal traffic density, we are tuning the TTL value to generate more hotspots and peaks no greater than BS's traffic density (although we can do it). In our proposed method, ANs' traffic is always equal to or greater than the BS's traffic; therefore the global adversary cannot infer BS location information on the basis of traffic analysis attack.

7 Conclusions

In a WSN, some applications, e.g., military, need privacy while some applications, e.g., agriculture, need energy conservation, and some applications need a hybrid approach (both privacy and energy). In MimiBS, for strong BS privacy, a high TTL value is recommended. It creates dense traffic to hide the BS location. The only energy winner is the SP algorithm, but it is not used practically to protect BS privacy. MimiBS provides BS station anonymity. It delivers packets quickly, while guarding against traffic analysis and tracing attacks. The balanced energy distribution guarantees network availability and prolonged life. For WSNs, the research is in progress to use pre-existing security parameters like burning cryptography key on chip, or software-defined cryptography. Leveraging the advantages of cloud computing, Internet of Things (IoT), virtualization, and software-defined networking, WSNs reshape to adopt the new set of architecture. Software-defined wireless sensor networks are the emerging and new set of architecture for traditional WSNs. Our future goal is to integrate traditional WSNs to the new paradigm of software-defined networking to provide better, scalable, flexible, and manageable architecture, and to provide a better privacy protection mechanism for BS.

Acknowledgment We are indebted to the anonymous reviewers whose insightful-comments, suggestions, and directions noticeably improved the quality of the paper.

References

[1] Satya Murty S A V, Raj B, Sivalingam K M, Ebenezer J, Chandran T, Shanmugavel M, Rajan K K. Wireless sensor network for sodium leak detection. *Nuclear Engineering and Design*, 2012, 249: 432-437.

[2] Bagula A. Applications of wireless sensor networks. http://wireless.ictp.it/wp-content/uploads/2012/02/WSN-Applications.pdf, February 2012.

[3] Lopez J, Zhou J. Wireless Sensor Network Security. Andreas Hermann, 2012.

[4] Mottola L, Picco G P. Programming wireless sensor networks: Fundamental concepts and state of the art. *ACM Computing Surveys*, 2011, 43(3): Article No. 19.

[5] Akyildiz I F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. *Computer Networks*, 2002, 38(4): 393-422.

[6] Diffie W, Landau S. Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press, 2007.

[7] Rios R, Lopez J. (Un)Suitability of anonymous communication systems to WSN. *IEEE Systems Journal*, 2013, 7(2): 298-310.

[8] Conti M, Willemsen J, Crispo B. Providing source location privacy in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials*, 2013, 15(3): 1238-1280.

[9] Pongaliur K, Xiao L. Sensor node source privacy and packet recovery under eavesdropping and node compromise attacks. *ACM Trans. Sensor Networks*, 2013, 9(4): Article No. 50.

[10] Proaño A, Lazos L. Perfect contextual information privacy in WSNs undercolluding eavesdroppers. In *Proc. the 6th ACM Conf. Security and Privacy in Wireless and Mobile Networks*, April 2013, pp.89-94.

[11] Long J, Dong M X, Ota K, Liu A F. Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks. *IEEE Access*, 2014, 2: 633-651.

[12] Rios R, Lopez J. Analysis of location privacy solutions in wireless sensor networks. *IET Communications*, 2011, 5(17): 2518-2532.

[13] Deng J, Han R, Mishra S. Countermeasures against traffic analysis attacks in wireless sensor networks. In *Proc. the 1st Int. Conf. Security and Privacy for Emerging Areas in Communications Networks*, September 2005, pp.113-126.

[14] Luo X, Ji X, Park M S. Location privacy against traffic analysis attacks in wireless sensor networks. In *Proc. Int. Conf. Information Science and Applications*, April 2010.

[15] Mehta K, Liu D G, Wright M. Protecting location privacy in sensor networks against a global eavesdropper. *IEEE Trans. Mobile Computing*, 2012, 11(2): 320-336.

[16] Ying B D, Gallardo J R, Makrakis D, Mouftah H T. Concealing of the sink location in WSNs by artificially homogenizing traffic intensity. In *Proc. IEEE Conf. Computer Communications Workshops*, April 2011, pp.988-993.

[17] Ebrahimi Y, Younis M. Using deceptive packets to increase base-station anonymity in wireless sensor network. In *Proc. the 7th Int. Wireless Communications and Mobile Computing Conf.*, July 2011, pp.842-847.

[18] Ying B D, Makrakis D, Mouftah H T. A protocol for sink location privacy protection in wireless sensor networks. In *Proc. IEEE Global Telecommunications Conf.*, December 2011.

[19] Gottumukkala V P V, Pandit V, Li H L, Agrawal D P. Base-station location anonymity and security technique (BLAST) for wireless sensor networks. In *Proc. IEEE Int. Conf. Communications*, June 2012, pp.6705-6709.

[20] Chen H L, Lou W. From nowhere to somewhere: Protecting end-to-end location privacy in wireless sensor networks. In *Proc. the 29th IEEE Int. Performance Computing and Communications Conf.*, December 2010.

[21] Bicakci K, Bagci I E, Tavli B. Lifetime bounds of wireless sensor networks preserving perfect sink unobservability. *IEEE Communications Letters*, 2011, 15(2): 205-207.

[22] Jian Y, Chen S, Zhang Z, Zhang L. Protecting receiver-location privacy in wireless sensor networks. In *Proc. the 26th IEEE INFOCOM*, May 2007, pp.1955-1963.

[23] Zhou L M, Wen Q Y. Energy efficient source location privacy protecting scheme in wireless sensor networks using ant colony optimization. *International Journal of Distributed Sensor Networks*, 2014, 2014: 920510.

[24] Goldschlag D, Reed M, Syverson P. Onion routing. *Communications of the ACM*, 1999, 42(2): 39-41.

[25] Kamat P, Zhang Y Y, Trappe W, Ozturk C. Enhancing source-location privacy in sensor network routing. In *Proc. the 25th IEEE Int. Conf. Distributed Computing Systems*, June 2005, pp.599-608.

[26] Braginsky D, Estrin D. Rumor routing algorithm for sensor networks. In *Proc. the 1st ACM Int. Workshop on Wireless Sensor Networks and Applications*, September 2002, pp.22-31.

[27] Eugster P T, Guerraoui R, Handurukande S B, Kouznetsov P, Kermarrec A M. Lightweight probabilistic broadcast. *ACM Trans. Computer Systems*, 2003, 21(4): 341-374.

[28] Kamat P, Xu W Y, Trappe W, Zhang Y Y. Temporal privacy in wireless sensor networks. In *Proc. the 27th Int. Conf. Distributed Computing Systems*, June 2007.

[29] Niu B, Zhu X Y, Li W H, Li H. EPcloak: An efficient and privacy-preserving spatial cloaking scheme for LBSs. In *Proc. the 11th IEEE Int. Conf. Mobile Ad Hoc and Sensor Systems*, October 2014, pp.398-406.

[30] Shao J, Lu R X, Lin X D. FINE: A fine-grained privacy-preserving location-based service framework for mobile devices. In *Proc. IEEE INFOCOM*, April 2014, pp.244-252.

[31] Latha K, Jayanthi S, Elavenil V. KRUPTO: Supporting privacy against location dependent attacks in wireless sensor network. In *Proc. Int. Conf. Communications and Signal Processing*, April 2013, pp.908-912.

[32] Shu T, Chen Y Y, Yang J, Williams A. Multi-lateral privacy-preserving localization in pervasive environments. In *Proc. IEEE INFOCOM*, April 27-May 2, 2014, pp.2319-2327.

[33] Xing K, Wan Z G, Hu P F, Zhu H J, Wang Y P, Chen X, Wang Y, Huang L S. Mutual privacy-preserving regression modeling in participatory sensing. In *Proc. IEEE INFOCOM*, April 2013, pp.3039-3047.

[34] Shafiei H, Khonsari A, Derakhshi H, Mousavi P. Rate-privacy in wireless sensor networks. In *Proc. IEEE Conf. Computer Communications Workshops*, April 2013, pp.67-68.

[35] Rana S S, Vaidya N H. A new 'Direction' for source location privacy in wireless sensor networks. In *Proc. IEEE Global Communications Conf,*, December 2012, pp.342-347.

[36] Ren J, Li Y, Li T T. Providing source privacy in mobile ad hoc networks. In *Proc. the 6th IEEE Int. Conf. Mobile Adhoc and Sensor Systems*, October 2009, pp.332-341.

[37] Wang W, Zhang Q. A stochastic game for privacy preserving context sensing on mobile phone. In *Proc. IEEE INFOCOM*, April 27-May 2, 2014, pp.2328-2336.

[38] Li Q H, Cao G H. Providing efficient privacyaware incentives for mobile sensing. In *Proc. the 34th IEEE Int. Conf. Distributed Computing Systems*, June 3-July 3, 2014, pp.208-217.

[39] Qiu F D, Wu F, Chen G H. SLICER: A slicing-based k-anonymous privacy preserving scheme for participatory sensing. In *Proc. the 10th IEEE Int. Conf. Mobile Ad-Hoc and Sensor Systems*, October 2013, pp.113-121.

[40] Yi Y Q, Li R, Chen F, Liu A X, Lin Y P. A digital watermarking approach to secure and precise range query processing in sensor networks. In *Proc. IEEE INFOCOM*, April 2013, pp.1950-1958.

[41] Jose J, Princy M, Jose J. EPSDA: Energy efficient privacy preserving secure data aggregation for wireless sensor networks. *International Journal of Security and Its Applications*, 2013, 7(4): 299-316.

[42] Dutta R, Gupta S, Paul D. Energy efficient modified SPIN protocol with high security in wireless sensor networks using TOSSIM. In *Proc. Int. Conf. Parallel Distributed and Grid Computing*, December 2014, pp.290-294.

[43] Liu Z, Seo H, Kim H. A synthesis of multiprecision multiplication and squaring techniques for 8-bit sensor nodes: State-of-theart research and future challenges. *Journal of Computer Science and Technology*, 2016, 31(2): 284-299.

[44] Oliveira C A S, Pardalos P M. Mathematical Aspects of Network Routing Optimization. Springer, 2011.

[45] Matsumoto M, Nishimura T. Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Modeling and Computer Simulation*, 1998, 8(1): 3-30.

[46] Romer K, Mattern F. The design space of wireless sensor networks. *IEEE Wireless Communications*, 2004, 11(6): 54-61.

[47] Barad J, Kadhiwala B. DIST-LEACH: A deterministic key management scheme for securing cluster-based sensor networks. In *Proc. Int. Conf. Advances in Engineering and Technology Research*, August 2014.

[48] Anastasi G, Falchi A, Passarella A, Conti M, Gregori E. Performance measurements of motes sensor networks. In *Proc. the 7th ACM Int. Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems*, October 2004, pp.174-181.

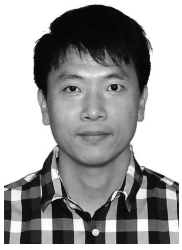
[49] Xiao W C, Zhang H, Wen Q Y, Li W M. Passive RFID-supported source location privacy preservation against global eavesdroppers in WSN. In *Proc. the 5th IEEE Int. Conf. Broadband Network & Multimedia Technology*, November 2013, pp.289-293.

[50] Reh F J. Pareto's principle — The 80-20 rule. *Business Credit*, 2005, 107(7): 76.

[51] Tudose D, Gheorghe L, Tapus N. Radio transceiver consumption modeling for multi-hop wireless sensor networks. *UPB Scientific Bulletin Series C*, 2013, 75(1): 17-26.

[52] Fu W H, Wang X Y, Agrawal D P. Multisubnets selection and rate allocation in a heterogeneous wireless network. In *Proc. the 7th IEEE Int. Conf. Mobile Adhoc and Sensor Systems*, November 2010, pp.715-720.

Yawar Abbas Bangash received his B.S. degree in software engineering from North West Frontier Province (NWFP) University of Engineering and Technology Peshawar, Mardan Campus, in 2008. From 2008 to 2012, he worked in Huawei Organization Pakistan Ltd., Higher Education Commission project (HEC) PERN2, and Baluchistan Education Foundation (BEF) on different positions in computer networking sector. In 2014 he got his M.S. degree in computer engineering from Wuhan University of Technology, Wuhan. In 2017, he received his Ph.D. degree from Huazhong University of Science and Technology (HUST), Wuhan. His research interests include security in WSN, software-defined technologies, and security in data communication for software-defined storage.



Ling-Fang Zeng received his B.S. degree in applied computer from Huazhong University of Science and Technology (HUST), Wuhan, in 2000, his M.S. degree in applied computer from China University of Geosciences, Wuhan, in 2003, and his Ph.D. degree in computer architecture from HUST, Wuhan, in 2006. He was a research fellow for four years in Department of Electrical and Computer Engineering, National University of Singapore, Singapore, during 2007∼2008 and 2010∼2013. He is currently with Wuhan National Laboratory for Optoelectronics, and School of Computer Science and Technology, HUST, as an associate professor. He has published more than 50 papers in major journals and conferences, including ACM Transactions on Storage, IEEE Transactions on Magnetics, Journal of Parallel and Distributed Computing, Journal of Network and Computer Applications, Software: Practice and Experience, FAST, SC, MSST, IPDPS, CLUSTER, and CCGrid, and serves for multiple international journals and conferences. He is a member of CCF, ACM, and IEEE.

Dan Feng received her B.E., M.E., and Ph.D. degrees in computer science and technology from Huazhong University of Science and Technology (HUST), Wuhan, in 1991, 1994, and 1997, respectively. She is a professor and the dean of the School of Computer Science and Technology, HUST, Wuhan. Her research interests include computer architecture, massive storage systems, and parallel file systems. She has over 100 publications in journals and international conferences, including FAST, ICDCS, HPDC, SC, ICS, and ICPP. Dr. Feng is a member of CCF, ACM, and IEEE.