Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 7, July-2017

Clone Detection in Wireless Sensor Network by energy and memory efficiently

Amrutha Varshini A S[1], Smt. G Anitha[2]

[1]PG Student, University BDT College of Engineering, Visveswaraya Technological University, Hadadi Road, Davangere, Karnataka, India.

[2]Associate Professor, University BDT College of Engineering, Visveswaraya Technological University, Hadadi Road, Davangere, Karnataka, India.

DOS in Computer Science and Engineering

Abstract: In this paper, we propose an energy-efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 per cent clone detection probability with trustful witnesses. It is easy for adversaries to mount node replication attacks due to the unattended nature of wireless sensor networks. In several replica node detection schemes, witness nodes fail to work before replicas are detected due to the lack of effective random verification. Our scheme distributes node location information to multiple randomly selected cells and then linear-multicasts the information for verification from the localized cells. Simulation results show that the proposed protocol improves detection efficiency compared with various existing protocols and prolongs the lifetime of the overall network. Extensive simulations demonstrate that our proposed protocol can achieve long network lifetime by effectively distributing the traffic load across the network.

Keywords: Wireless sensor networks, clone detection protocol, energy efficiency, network lifetime

I. INTRODUCTION

Wireless sensor networks are known as one of the three high-tech industries in the new century due to their great promise and potential with their various applications, such as in military affairs, industrial production, and environmental monitoring. Now, more and more security requirements continue to arise due to the wide application and the popularization of wireless sensor networks. The ease of deploying sensor networks improves their appeal. One sensor node can be easily inserted into an arbitrary location in a wireless sensor network without triggering any intervention from the administrator and interaction with the base station. In fact, the intrusion is only realized by triggering a simple neighbour discovery protocol. On the other hand, sensor nodes deployed in an unattended environment lack prior knowledge and hardware shielding, which is advantageous for an adversary who wants to capture and comprise them. Due to the simple structure of the sensor node, once the attacker captures one or more of the sensor nodes in the network, the running program can be cracked through a reverse analysis technique.

To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection [11]. The first requirement is to make it difficult for malicious users eavesdrop the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages. The second requirement is to make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not. To

guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfill these requirements in clone detection protocol design.

In this paper, besides the clone detection probability, we also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness selection scheme in WSNs. Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to launch attacks. A preliminary work is presented in [1]. In that work, we proposed an energy-efficient ring based clone detection (ERCD) protocol to achieve high clone detection probability with random witness selection, while ensuring normal network operations with satisfactory network lifetime of WSNs. The ERCD protocol can be divided into two stages: witness selection and legitimacy verification. In witness selection, the source node sends its private information to a set of witnesses, which are randomly selected by the mapping function. In the legitimacy verification, verification message along the private information of the source node is transmitted to its witnesses. If any of witnesses successfully receives the message, it will forward the message to its witness header for verification. Upon receive the messages, the witness header compares the aggregated verification messages with stored records. If multiple copies of verification messages are received, the clone attack is detected and a revocation procedure will be triggered. As such, to have a comprehensive study of the ERCD protocol, we extend the analytical model by evaluating the required data buffer of ERCD protocol and by including experimental results to support our theoretical analysis. First, we theoretically prove that our proposed clone detection protocol can achieve probability 1 based on trustful witnesses. Considering the scenario that witnesses can be compromised, our simulation results demonstrate that the clone detection probability can still approach 98 percent in WSNs with 10 percent cloned nodes by using the ERCD protocol. Second, to evaluate the performance of network lifetime, we derive the expression of total energy consumption, and then compare our protocol with existing clone detection protocols. We find that the ERCD protocol can balance the energy consumption of sensors at different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings around the sink, which should not have witnesses. After that, we obtain the optimal number of non-witness rings based on the function of energy consumption. Finally, we derive the expression of the required data buffer by using ERCD protocol, and show that our proposed protocol is scalable because the required buffer storage is dependent on the ring size only. Extensive simulation results demonstrate that our proposed ERCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.

II. LITERATURE SURVEY

As one of the utmost important security issues, clone attack has attracted people's attention. There are many works [14], [15], [16] that studies clone detection protocols in the literature, which can be classified into two different categories, i.e., centralized and distributed clone detection protocols. In centralized protocols, the sink or witnesses generally locate in the center of each region, and store the private information of sensors. When the sink or witnesses receive the private information of the source node, they can determine whether there is a clone attack by comparing the private information with its pre-stored records [17], [18]. Normally, centralized clone detection protocols have low overhead and running complexity. However, the security of sensors' private information may not be guaranteed, because the malicious users can eavesdrop the transmission between the sink node and sensors. Moreover, the network lifetime may be dramatically decreased since the sensor nodes close to the sink will deplete their energy sooner than other nodes.

The general concept and the main idea of the centralized solution were described for the first time in the paper by Parno et al. [3]. According to this paper, there are several drawbacks inherent to a centralized system. First, the trusted third party (e.g., base station) plays an important role in the clone node detection. The base station is more likely to be compromised and to fall into a single-point failure. Second, the nodes surrounding the base station bear large amounts of the routing load. Adversaries may block the tunnel of the communication, and thus circumvent detection. Meanwhile, the power of those nodes is used up, so the lifespan of the network is shortened. Finally, for many networks, there is no powerful base station due to its high cost, so it is necessary to apply a distribution solution.

However, the randomness of mapping function also increases the difficulty for the source node to reach its witnesses, which makes it challenging to achieve a high clone detection probability. To ensure the clone detection probability, LSM lets all the nodes in the route between source and witnesses store the private information of the source node, which leads to a high requirement of data buffer and energy consumption. Thus, it is essential to guarantee the clone detection probability with low energy consumption and required buffer storage in clone detection protocols with random witness selection approach. Other distributed clone detection protocols, such as Parallel Multiple Probabilistic Cells (P-MPC), proposed semi-random witness selection approach [13],[19], trying to combine the advantages of both random and deterministic witness selection approaches. In this kind of witness selection scheme, a deterministic region is generated for the source node according to the mapping function, and then witnesses of the source node will be randomly selected from the sensors in this region. However, the two phases witness selection and randomness of the witnesses for each

sensor leads to a high overhead and time complexity. The energy consumption and the required buffer storage of such protocols are lower than the random witness selection approach but higher than the deterministic ones. Overall, most previous works aim at maximizing the clone detection probability without considering the impact of proposed clone detection protocol on the network lifetime and required data buffer storage. In this paper, we carefully design a distributed clone detection protocol with random witness selection by jointly considering the clone detection probability, network lifetime and data buffer capacity.

III. PROPOSED SYSTEM

In this paper, besides the clone detection probability, we also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness selection scheme in WSNs. Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to launch attacks. We extend the analytical model by evaluating the required data buffer of ERCD protocol and by including experimental results to support our theoretical analysis. Energy-Efficient Ring Based Clone Detection (ERCD) protocol. We find that the ERCD protocol can balance the energy consumption of sensors at different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings around the sink, which should not have witnesses. After that, we obtain the optimal number of non-witness rings based on the function of energy consumption.

Finally, we derive the expression of the required data buffer by using ERCD protocol, and show that our proposed protocol is scalable because the required buffer storage is dependent on the ring size only.

ADVANTAGES OF PROPOSED SYSTEM:

The performance of the ERCD protocol is evaluated in terms of clone detection probability, power consumption, network lifetime, and data buffer capacity.

Extensive simulation results demonstrate that our proposed ERCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.

The experiment results demonstrate that the clone detection probability can closely approach 100 per cent with untrustful witnesses.

By using ERCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection.

IV. SYSTEM ARCHITECTURE:

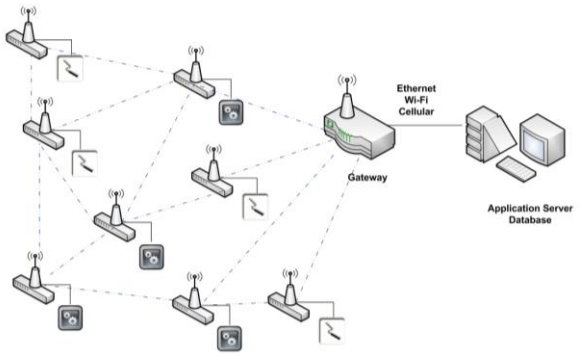

Fig. system architecture

V. IMPLIMENTATION

A. SYSTEM CONSTRUCTION MODULE:

In the first module, we develop the System Construction Module, to evaluate and implement our proposed system. In this module, we consider a network region with one base station (BS) and an enormous number of wireless sensor nodes randomly distributed in the network. We use the sink node as the origin of the system coordinator. Based on the location of the BS, the network region is virtually separated into adjacent rings, where the width of each ring is the same as the transmission range of sensor nodes. The network is a densely deployed WSN, i.e., i) for each node, there exist sensor nodes located in each neighboring ring, and ii) for each ring, in each ring, there are enough sensor nodes to construct a routing path along the ring.

B. ERCD PROTOCOL

In this module, we introduce our distributed clone detection protocol, namely ERCD protocol, which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity. The ERCD protocol consists of two stages: witness selection and legitimacy verification. In witness selection, a random mapping function is employed to help each source node randomly select its witnesses. In the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the private information of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages are different from existing record or the messages are expired, the witness header will report a clone attack to the sink to trigger a revocation procedure.

C. PROBABILITY OF CLONE DETECTION

In this module, we focus on designing a distributed clone detection protocol with random witness selection by jointly considering clone detection probability, network lifetime and data buffer storage. Initially, a small set of nodes are compromised by the malicious users. Utilizing the clone detection protocol, we aim at maximizing the clone detection probability, i.e., the probability that cloned node can be successfully detected, to ensure the security of WSNs; meanwhile, the sufficient energy and buffer storage capacity for data collection and operating clone detection protocol should be guaranteed, which means that the network lifetime, i.e., the period from the start of network operation until the first outage occurs, should not be impacted by the proposed clone detection protocol with sensors' buffer storage.
In distributed clone detection protocol with random witness selection, the clone detection
Probability generally refers to whether witnesses can successfully receive the verification message from the source node or not. Thus, the clone detection probability of ERCD protocol is the probability that the verification message can be successfully transmitted from the source node to its witnesses.

D. ENERGY CONSUMPTION AND NETWORK LIFETIME

In WSNs, since wireless sensor nodes are usually powered by batteries, it is critical to evaluate the energy consumption of sensor nodes and to ensure that normal network operations will not be broken down by node outage. Therefore, we define the network lifetime as the period from the start of network operation until any node outage occurs to evaluate the performance of the ERCD protocol.

We only consider the transmission power consumption, as the reception power consumption occupies little percentage of total power consumption. Since witness sets in our ERCD protocol are generated based on ring structure, sensor nodes in the same ring have similar tasks. To simplify the analysis, we suppose that all sensor nodes in the same ring have same traffic load.

Our analysis in this work is generic, which can be applied to various energy models. A node inside (outside) ring k refers to the node which locates in the ring with index smaller than (larger than) k. First, we analyze the traffic load of each sensor node, such that the energy consumption and network lifetime can be derived based on it. By using the ERCD protocol, traffic load of each sensor node consists of normal data collection, witness selection and legitimacy verification.

E. ALGORITHM:

TABLE 1
Notation List
h- The hop number of network radius
ha -The hop length from a to the sink
n -The number of nodes in the network
ni- The number of nodes in i-th ring
r- The transmission range of a node
Oa- The ring index of a
Owa-The witness ring index of a
Wa -The set of a's witness
Wa- One of a's witness in Wa
Sa- The witness header of Wa
IDa -The identity information of a
La- The location a claims to occupy
Ta- The timer of a's verification
Ka-The message including a's private information.

ALGORITHM STEPS:

Step1: Start the process.
Step2: Initialize the System Base station and Nodes of the network.
Step3: Next Broadcast the nodes, Paths are created.
Step4: After this path, verify the Connection of the path setting.
Step5: If verification is success then send the message.
Step6: If it's not success then find the clone. Then go back to the step2.
Step7: After this clone detection, the clone system can be blocked and send the message in the other path.
Step8: Stop the process.

VI. RESULTS

We study the impact of the duty cycle on the proposed ERCD protocol, and evaluate average delay and routing success rate, i.e., the rate of successful routing over all rounds of transmission, with various duty cycles. Specifically, we consider a WSN located in a 500 m _ 500 m region, where the transmission range of each sensor node is 50 m. In ERCD protocol, a sensor node will forward the message to another awaken sensor when available. If its neighboring sensors are in sleep mode, the sensor will hold the message till at least one relaying sensor wakes up or delay times out. The round of clone detection routing is determined as failure if the delay of any node's transmission is larger than 1 second. We evaluate the impact of duty cycle, denoted as t, on our protocol in terms of routing success rate. As shown in Fig. 15, based on a WSN with node density of 1:4_1:8 nodes/m2, the routing success rate increases with the growth of duty cycle and network density in general, due to more awaken sensors ready for forwarding.

We compare the network lifetime with different numbers of sensor nodes in Fig. 1. Generally, sensor nodes closer to the sink node have relatively heavier traffic load than those far away nodes, and will deplete their energy faster. With the growth of the node number, the traffic load of those sensors increases dramatically, which leads to a much shorter lifetime of those nodes. ERCD protocol distributes the traffic load across the network, which balances the energy consumption of sensors at different locations. Therefore, the proposed ERCD protocol achieves the best network lifetime among the listed protocols, and it does not significantly decrease with the increase of node number as shown in Fig. 1. The energy consumption of each step by using ERCD or some existing protocols is shown in Fig.2.

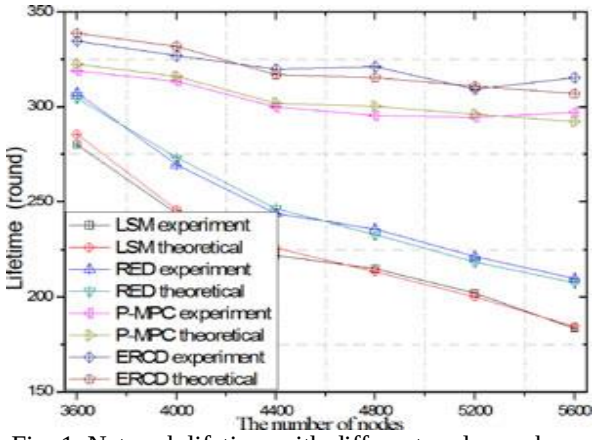

Fig. 1. Network lifetime with different node numbers.

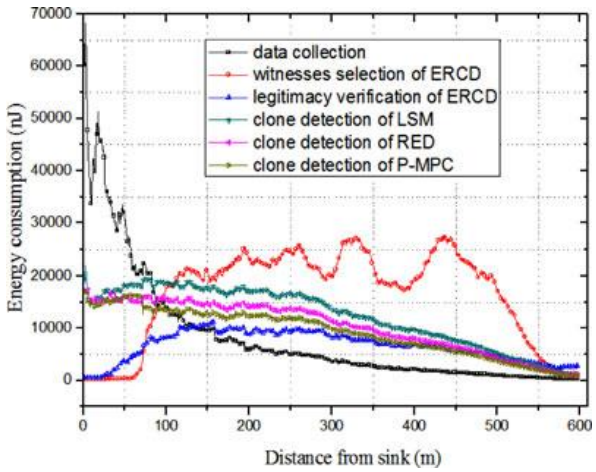

Fig.2. Energy consumption of each step by using ERCD or existing protocols.

We calculate energy consumption of ERCD protocol in data collection, witness selection and legitimacy verification, and that of LSM, RED and P-MPC in data collection and clonedetection. The energy consumption of data collection for all protocols is the same. In LSM, RED and P-MPC protocols, sensors close to the sink need to relay more traffic of both data collection and clone detection, thus have higher energy consumption and may have higher outage probability around the sink. By using ERCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection. The relationship of average delay, duty cycle and node density is shown in Fig. 16. The average delay is very small when node density is larger than 1.8 nodes/m2, and the average delay of sensor nodes decreases significantly with the increase of duty cycles from 0 to 0.05. based on a WSN with node density of 1:41:8 nodes/m2, the routing success rate increases with the growth of duty cycle and network density in general, due to more awaken sensors ready for forwarding.

VII. CONCLUSION

In this paper, we have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended. In our future work, we will consider different mobility patterns under various network scenarios.

REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.
[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emergingmachine to machine communications," IEEE Commun.Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.
[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.
[4] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.
[5] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.
[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 1036–1045, Sep. 2010.
[7] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.
[8] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, May. 2011.
[9] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.
[10] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.
[11] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, Oakland, CA, USA, May. 8-11, 2005, pp. 49–63.
[12] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.
[13] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.
[14] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 793–806, May. 2012.
[15] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen., "BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 32–43, Jan. 2012.
[16] J. Li, J. Chen, and T. H. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors," in Proc. IEEE INFOCOM, Orlando, FL, USA, Mar. 25-30, 2012, pp. 118–126.
[17] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, Cybern., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.
[18] W. Naruephiphat, Y. Ji, and C. Charnsripinyo, "An area-based approach for node replica detection in wireless sensor networks," in Proc. IEEE TrustCom, Liverpool, UK, Jun. 25-27, 2012, pp. 745–750.
[19] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proc. IEEE 17th Int. Conf. Netw. Protocols, Princeton, NJ, USA, Oct. 13-16, 2009, pp. 284–293.
[20] T. Bonaci, P. Lee, L. Bushnell, and R. Poovendran, "Distributed clone detection in wireless sensor networks: An optimization approach," in Proc. IEEE IEEE Int. Symp. World of Wireless, Mobile Multimedia Netw., Lucca, IT, Jun. 20-23, 2011, pp. 1–6.
[21] Q. Chen, S. S. Kanhere, and M. Hassan, "Analysis of per-node traffic load in multi-hop wireless sensor networks," IEEE Trans. Wireless Commun., vol. 8, no. 2, pp. 958–967, Feb. 2009.
[22] A. Liu, P. Zhang, and Z. Chen, "Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks," J. Parallel Distrib. Comput., vol. 71, no. 10, pp. 1327–1355, Oct. 2011.
[23] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. Security Privacy, Berkeley, CA, USA, May 11-14, 2003, pp. 197–213.
[24] C. Ok, S. Lee, P. Mitra, and S. Kumara, "Distributed routing in wireless sensor networks using energy welfare metric," Inf. Sci., vol. 180, no. 9, pp. 1656–1670, May 2010.
[25] OMNET++ network simulation framework:[Online].Available:http://www.omnetpp.org/