ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Filtering Injected False Data in Wireless Sensor Networks by Using L, F, S Nodes and Key Distribution

Amuthan Mathy.P[1], Gowri Sankar.U[2]

PG Scholar, V.S.B Engineering College[1]

Assistant Professor, V.S.B Engineering College[2]

ABSTRACT: To achieve security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent between sensor nodes. Many key agreement schemes used in general networks, such as public-key based schemes, are not suitable for wireless sensor networks due to the limited computational abilities of the sensor nodes. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory this requires when the network size is large. In this paper, we provide a framework in which to study the security of key pre-distribution schemes, propose a new key pre-distribution scheme which substantially improves the resilience of the network compared to previous schemes, and give an in-depth analysis of our scheme in terms of network resilience and associated overhead. when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is close to zero. This desirable property lowers the initial payoff of smaller-scale network breaches to an adversary, and makes it necessary for the adversary to attack a large fraction of the network before it can achieve any significant gain.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support. Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. To achieve this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications. Wireless sensor networks are deployed to monitor the sensing field and gather information from it. Traditionally, two approaches can be adopted to accomplish the data collection task: through direct communication, and through multi-hop forwarding. In the first case, sensor nodes upload data directly to the sink through one-hop wireless communication, which may result in long communication distances and degrade the energy efficiency of sensor nodes. On the other hand, with multi-hop forwarding, data are reported to the sink through multiple relays, and the communication distance is reduced. However, since nodes near the sink generally have a much heavier forwarding load, their energy may be depleted very fast, which degrades the network performance.

II. NATURES OF ROUTING

Since a distributed network has multiple nodes and services many messages, and each node is a shared resource, many decisions must be made. There may be multiple paths from the source to the destination. Therefore, message routing is an important topic. The main performance measures affected by the routing scheme are throughput (quantity of service) and average packet delay (quality of service). Routing schemes should also avoid both deadlock and live lock (see below). Routing methods can be fixed (i.e. pre-planned), adaptive, centralized, distributed, broadcast, etc. Perhaps the simplest routing scheme is the token ring [Smythe 1999]. Here, a simple topology and a straightforward fixed protocol result in very good reliability and pre computable QoS. A token passes continuously around a ring topology. When a node desires to transmit, it captures the token and attaches the message. As the token passes, the destination reads the header, and captures the message. In some schemes, it attaches a 'message received' signal to the token, which is then received by the original source node. Then, the token is released and can accept further messages. The token ring is a completely decentralized scheme that effectively uses TDMA. Though this scheme is very reliable, one can see that it results in a waste of network capacity. The token must pass once around the ring for each message. Therefore, there are various modifications of this scheme, including using several tokens, etc. Fixed routing schemes often use Routing Tables that dictate the next node to be routed to, given the current message location and the destination node. Routing tables can be very large for large networks, and cannot take into account real-time effects such as failed links, nodes with backed up queues, or congested links. Adaptive routing schemes depend on the current network status and can take into account various performance measures, including cost of transmission over a given link, congestion of a given link, reliability of a path, and time of transmission. They can also account for link or node failures.

III. ROUTING PROTOCOL

Routing has two main functions: route discovery and packet forwarding. The former is concerned with discovering routes between nodes, whereas the latter is about sending data packets through the previously discovered routes. There are different types of ad hoc routing protocols. One can distinguish proactive and reactive protocols. Protocols of the latter category are also called on-demand protocols. Another type of classification distinguishes routing table based protocols (e.g., DSDV) and source routing protocols (e.g., DSR).

IV. GENERAL PROJECT DETAILS

A wireless sensor network (WSN) is usually composed of several resource-limited sensor nodes, which can work collaboratively and deliver useful information to users upon queries and events. Since sensor nodes may collect sensitive information, security and privacy become a concern that cannot be ignored .Moreover, several real-world scenarios, including community/environment monitoring, smart home, need data transmitted over the network and data stored in nodes' memories. Due to the resource-limited sensor nodes, traditional network security mechanisms are not suitable for WSNs. Inspired by the above challenges, we study the issues of secure network protocol and data access control in WSNs in order to avoid data leaking to the adversary or unauthorized party. Security services such as authentication and key establishment are critical to sensor networks. They enable sensor nodes to communicate securely with each other using cryptographic techniques. However, recent research works have suggested that connectivity and lifetime of a sensor network can be substantially improved if some nodes are given greater power and transmission capability. Therefore, how to exploit those heterogeneity features in design of a good distributed key management scheme has become an important issue. As our work, we propose two key pre-distribution schemes that enable a sink or leader node to establish a secure data communication link, on the fly, with any sensor nodes.

A wireless sensor network (WSN) is usually composed of several resource-limited sensor nodes, which can work collaboratively and deliver useful information to users upon queries and events. Since sensor nodes may collect sensitive information, security and privacy become a concern that cannot be ignored. Moreover, several real-world scenarios, including community/environment monitoring, smart home, need data transmitted over the network and data stored in nodes' memories. Due to the resource-limited sensor nodes, traditional network security mechanisms are not suitable for WSNs. Inspired by the above challenges, we study the issues of secure network protocol and data access control in WSNs in order to avoid data leaking to the adversary or unauthorized party.

Security services such as authentication and key establishment are critical to sensor networks. They enable sensor nodes to communicate securely with each other using cryptographic techniques. However, recent research works have suggested that connectivity and lifetime of a sensor network can be substantially improved if some nodes are given greater power and transmission capability. Therefore, how to exploit those heterogeneity features in design of a good distributed key management scheme has become an important issue. As our work, we propose two key pre-distribution schemes that enable a sink or leader node to establish a secure data communication link, on the fly, with any sensor nodes.

V. POLYNOMIAL AND GENERATION KEY SUBSETS ASSIGNMENTS

The proposed schemes are based on the polynomial pool based key pre-distribution scheme. The security analysis in this work indicates that the proposed pre distribution schemes assure, with high probability and low communication overhead, that any sensor node can establish a pairwise key with the sink.

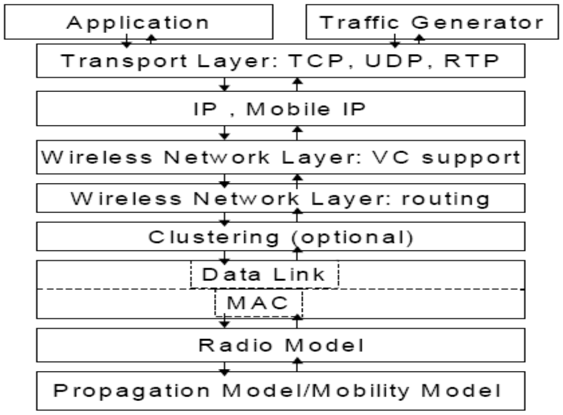
Their relationship is illustrated in above Fig. There are three types of nodes, including leader node (LN), function node (FN), and sensor node (SN), in our sensor network topology. The network region is partitioned into physical clusters, each of which contains a FN in charge of SNs in that cluster. In each cluster, SNs are responsible for collecting sensed data, while FNs aggregate the data from SNs; send commands to SNs; keep utility data, appliances, etc. in inside memory; and forward the received data to their upper level nodes (i.e., LNs, FNs).

The LN is a network owner with abundant resources that can query data by an on-demand wireless link connected to all FNs. To prevent storage overflow of FNs, the LN can also be periodically dispatched to collect data and empty the storage of FNs.

To keep the confidentiality of messages transmitted over the network, there are two types of keys, common keys (used for FN/FNs to broadcast packet) and pairwise keys (used for each FN/SNs), used in our system. Here, the common key is distributed in advance by leader node or sink node. After sensor deployment, pairwise keys are constructed for each cluster with respect to FN of sensor nodes by applying our scheme.

Security analyses indicate that the proposed schemes provide a higher probability for non-compromised sensors to establish a secure communication with the sink than previous schemes. Our scheme is able to achieve the goals of much less energy consumption and higher security than previous works.

GloMoSim is a scalable simulation library for wireless network Systems built using the Parsec simulation environment. In contrast to existing network simulators such as OPNET and NS, GloMoSim has been designed and built with the primary goal of simulating very large network models that can scale up to a million nodes using parallel simulation to significantly reduce execution times of the simulation model. As most network systems adopt a layered approach similar to the OSI seven layer network architecture. Simple APIs are defined between different similar simulation layers. This allows the rapid integration of models developed at different layers by different people.


Application
Traffic Generator
Transport Layer: TCP, UDP, RTP
IP , Mobile IP
Wireless Network Layer: VC support
Wireless Network Layer: routing
Clustering (optional)
Data Link
MAC
Radio Model
Propagation Model/Mobility Model

Glomosim Architecture

GloMoSim is a scalable simulation library for wireless network Systems built using the Parsec simulation environment. GloMoSim also supports two different node mobility models. Nodes can move according to a model that is generally referred to as "random waypoint". A node chooses a random destination within the simulated terrain and moves to that location based on the speed specified in the configuration file. After reaching its destination, the node pauses for a duration that is specified in the configuration file. The other mobility model in the GloMoSim is referred to as the "random drunken" model. A node periodically moves to a position chosen randomly from its immediate neighboring positions. The frequency of the change in node position is based on a parameter specified in the configuration file.

In contrast to existing network simulators such as OPNET and NS, GloMoSim has been designed and built with the primary goal of simulating very large network models that can scale up to a million nodes using parallel simulation to significantly reduce execution times of the simulation model. As most network systems adopt a layered approach similar to the OSI seven layer network architecture. Simple APIs are defined between different similar simulation layers. This allows the rapid integration of models developed at different layers by different people.

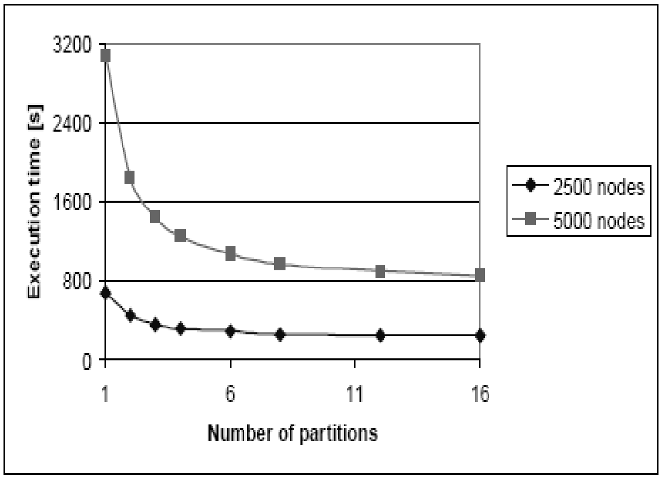
VI. GLOMOSIM LIBRARY

GloMoSim is a scalable simulation library for wireless network systems built using the PARSEC simulation environment.

Scalability of GloMoSim

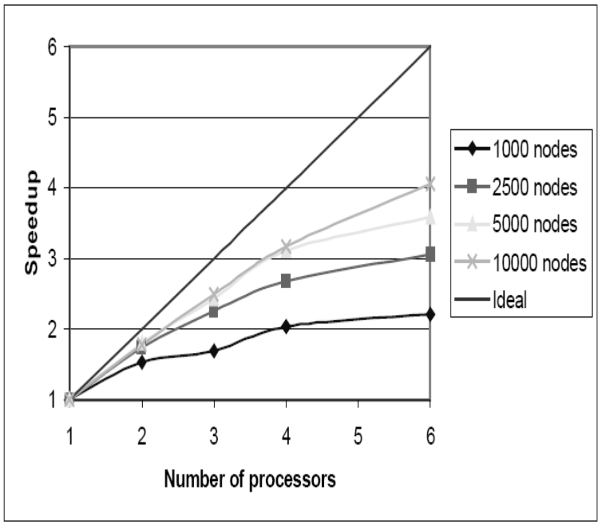
The node aggregation technique gives significant benefits to the simulation performance. As each entity needs to examine packet receptions only for the nodes located in the region it is simulating, using many partitions reduce the total search space for packet delivery. Fig.5.2 ows the impact of multiple partitions for the models with 2500 and 5000 wireless nodes. Both simulation models consist of wireless nodes running CSMA at the MAC layer, each of which is randomly placed in 2000 x 2000m free space region. As seen in Fig.5.2, the executions for both models become faster as the number of partitions increases. The effect of multiple partitions is larger for the model with 5000 nodes as the reduction in the execution time is related to the number of wireless nodes to be examined for each radio transmission. GloMoSim is aimed at simulating models that may contain as many as 100,000 mobile nodes with a reasonable execution time. GloMoSim has already been used to simulate 10,000 nodes up to the MAC layer using parallel execution of the model on shared memory architectures. Indicates parallel performance of GloMoSim on a Sun SPARCserver 1000. Speedup rates are calculated based on the sequential execution of each model.

The same configuration as the experiments on multiple partitions is used with different number of wireless nodes. Twelve partitions are used for all the executions to balance the workload of each processor.



Execution times against the number of partitions.

GloMoSim achieved better parallel performance for models with higher number of wireless nodes because more activities occur concurrently in those models, which increase the parallelism of models. Users, especially those who need to simulate large-scale models can benefit from this parallel simulation capability of GloMoSim. It shows increases of execution times against the number of mobile nodes in the model. With the same number of processors, the execution time increases dramatically as the number of mobile nodes in the model increases. However, the execution time with 6 processors for the 10000 node model is shorter than the sequential execution for the 5000 node model. This implies that the user can run the simulation for a model consisting of twice the number of mobile node in the same amount of time with 6 processors. Parallel simulation requires synchronization of simulation clock among multiple processors. PARSEC simulation environment provides four variations of conservative protocols and an optimistic protocol for the synchronization. The current GloMoSim kernel has parallel execution directives for conservative protocols and will be capable of executing models using optimistic protocols in future. The experiments done in this section used the null message protocol, which is one of the most basic conservative protocols widely used for many applications.

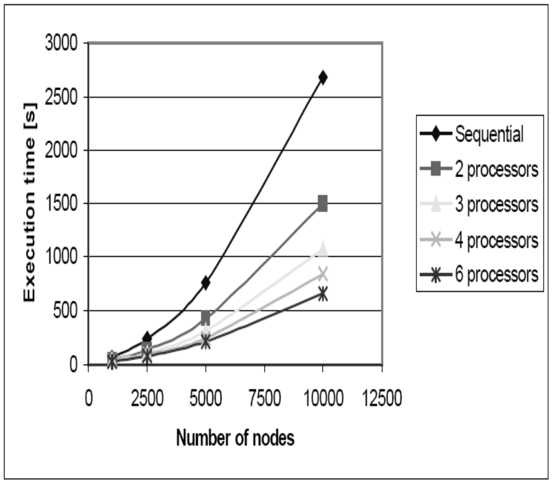


Parallel performance with different number of nodes

Visualization Tool

The primary purpose of the Java VT is to help network designers debug their protocols. It is written in Java to provide portability across
multiple platforms.

The GloMoSim simulation can be run with or without the VT. If run without the VT, it can just be executed from the command line. However, if run with the VT, it must be executed through the GUI provided by the VT rather than from the command line.



Execution times with varying number of nodes.

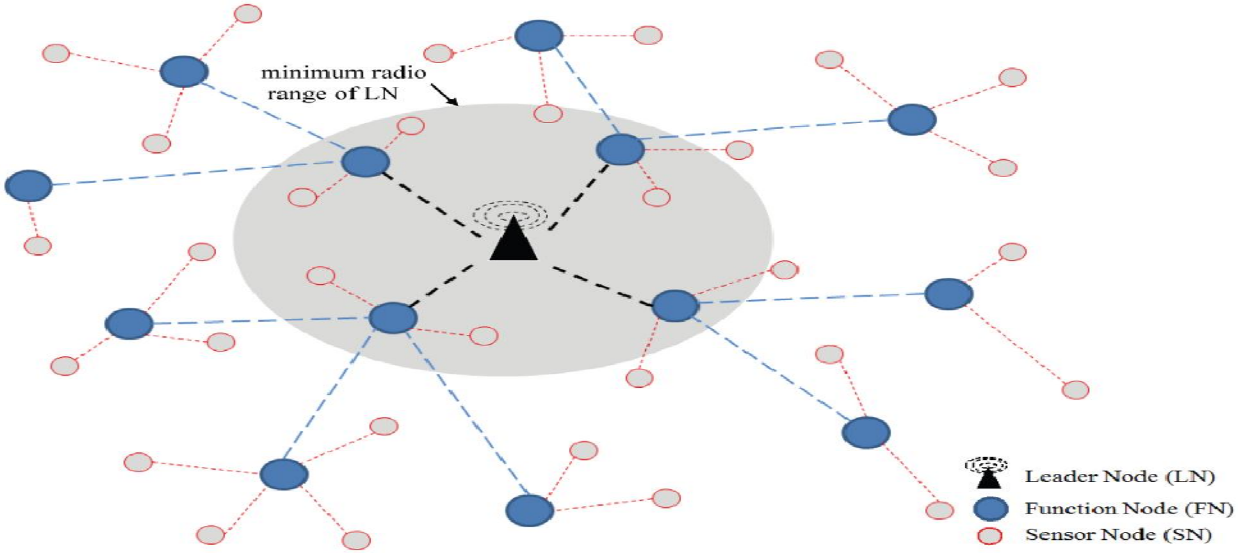
VII. SYSTEM SPECIFICATION

A wireless sensor network (WSN) is usually composed of several resource-limited sensor nodes, which can work collaboratively and deliver useful information to users upon queries and events. Since sensor nodes may collect sensitive information, security and privacy become a concern that cannot be ignored. Moreover, several real-world scenarios, including community/environment monitoring, smart home, need data transmitted over the network and data stored in nodes' memories. Due to the resource-limited sensor nodes, traditional network security mechanisms are not suitable for WSNs. Inspired by the above challenges, we study the issues of secure network protocol and data access control in WSNs in order to avoid data leaking to the adversary or unauthorized party.

Security services such as authentication and key establishment are critical to sensor networks. They enable sensor nodes to communicate securely with each other using cryptographic techniques. However, recent research works have suggested that connectivity and lifetime of a sensor network can be substantially improved if some nodes are given greater power and transmission capability. Therefore, how to exploit those heterogeneity features in design of a good distributed key management scheme has become an important issue. As our work, we propose two key pre-distribution schemes that enable a sink or leader node to establish a secure data communication link, on the fly, with any sensor nodes.

VIII. POLYNOMIAL AND GENERATION KEY SUBSETS ASSIGNMENTS

The proposed schemes are based on the polynomial pool based key pre-distribution scheme. The security analysis in this work indicates that the proposed pre distribution schemes assure, with high probability and low communication overhead, that any sensor node can establish a pairwise key with the sink.



Their relationship is illustrated in above Fig. There are three types of nodes, including leader node (LN), function node (FN), and sensor node (SN), in our sensor network topology. The network region is partitioned into physical clusters, each of which contains a FN in charge of SNs in that cluster. In each cluster, SNs are responsible for collecting sensed data, while FNs aggregate the data from SNs; send commands to SNs; keep utility data, appliances, etc. in inside memory; and forward the received data to their upper level nodes (i.e., LNs, FNs). The LN is a network owner with abundant resources that can query data by an on-demand wireless link connected to all FNs. To prevent storage overflow of FNs, the LN can also be periodically dispatched to collect data and empty the storage of FNs.

To keep the confidentiality of messages transmitted over the network, there are two types of keys, common keys (used for FN/FNs to broadcast packet) and pairwise keys (used for each FN/SNs), used in our system. Here, the common key is distributed in advance by leader node or sink node. After sensor deployment, pairwise keys are constructed for each cluster with respect to FN of sensor nodes by applying our scheme.

Security analyses indicate that the proposed schemes provide a higher probability for non-compromised sensors to establish a secure communication with the sink than previous schemes. Our scheme is able to achieve the goals of much less energy consumption and higher security than previous works.

IX. CONCLUSION

Key management has become a challenging issue in the design and deployment of secure wireless sensor networks. A common assumption in most existing distributed key management schemes is that all sensor nodes have the same capability. However, recent research works have suggested that connectivity and lifetime of a sensor network can be substantially improved if some nodes are given greater power and transmission capability. Therefore, how to exploit those heterogeneity features in design of a good distributed key management scheme (proposed method) has become an important issue. In this paper, we have proposed a novel bandwidth efficient cooperative authentication (BECAN) scheme for filtering the injected false data. By theoretical analysis and simulation evaluation, the BECAN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi reports.

Due to the simplicity and effectiveness, the BECAN scheme could be applied to other fast and distributed authentication scenarios, e.g., the efficient authentication in wireless mesh network. Ensuring the security of communication and access control in Wireless Sensor Networks (WSNs) is of paramount importance. In our future work, we will investigate how to prevent/mitigate the gang injecting false data attack from mobile compromised sensor nodes

REFERENCE

[1] R. Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An analysis of a large scale habit monitoring application," in ACM Sensys'04, 2004.
[2] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in ACM CCS'02, 2002.
[3] R. Lu, X. Lin, C. Zhang, H. Zhu, P. Ho, and X. Shen, "AICN: an efficient algorithm to identify compromised nodes in wireless sensor network," in Proc. IEEE ICC'08, Beijing, China, May 19-23 2008. [4] X. Lin, R. Lu, and X. Shen, "MDPA: multidimensional privacypreserving aggregation scheme for wireless sensor networks," Wireless Communications and Mobile Computing, vol. 10, pp. 843– 856, 2010.
[5] X. Lin, "CAT: Building couples to early detect node compromise attack in wireless sensor networks," in Proc. IEEE GLOBECOM'09, Honolulu, Hawaii, USA, Nov. 30 - Dec. 4 2009.
[6] K. Ren, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in Proc. IEEE SECON 2007, San Diego, Jue.18-21 2007.
[7] L. Zhou and C. Ravishankar, "A fault localized scheme for false report filtering in sensor networks," in International Conference on Pervasive Services, ICPS '05, July 2005, pp. 59–68.
[8] Z. Zhu, Q. Tan, and P. Zhu, "An effective secure routing for false data injection attack in wireless sensor network," in APNOMS 2007, vol. LNCS 4773. Springer-Verlag, 2007, pp. 457–465.
[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in IEEE Infocom'04, Hong Kong, China, March 7-11 2004.
[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-byhop authentication scheme for filtering of injected false data in sensor networks," in IEEE Symposium on Security and Privacy'04, 2004.
[11] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in Proc. of ACM MOBIHOC' 05, 2005, pp. 34 – 45.
[12] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," in Proc. IEEE INFOCOM 2006, Barcelona, Spain, Apr. 23-29 2006.
[13] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 247–260, 2006.
[14] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "A dos-resilient en-route filtering scheme for sensor networks," in MobiHoc '09: Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing. New York, NY, USA: ACM, 2009, pp. 343–344.
[15] J. Chen, Q. Yu, Y. Zhang, H.-H. Chen, and Y. Sun, "Feedback based clock synchronization in wireless sensor networks: A control theoretic approach," IEEE Transactions on Vehicular Technology, vol. 59, no. 6, pp. 2963–2973, June 2010.