IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 6, Ver. II (Nov.-Dec .2016), PP 26-32
www.iosrjournals.org

Digital Signature with Acknowledgement Based Clone Detection for wsns

P.Balasubramani[1], S.Maria Antony[2], G.SathishKumar[3] R.Krishnaveni[4] B.Priyadharshini[5]

Assistant ProfessorDepartment of Electronics and Communication EngineeringKIT-Kalaignarkarunanidhi Institute of Technology Coimbatore-641 402

Abstract: *The main objective of this paper is to improve the network security in hostile environment by detecting the clone nodes.Hence malicious nodes accessing the secret information isavoided. In this paper, duplicate node detection approach followed by clone nodes deduction was proposed for wireless sensor network(WSNs) and it is found to be working efficiently. Static sensor network based implementation calledTime Deployment Approach (TDA) is designed and compared with the former approaches. The work also focused on energy savings of both static sensor network as well as mobile sensor network.*

Index Terms: *Wireless Sensor Network(WSNs) Digital Signature Algorithm(DSA), network security, duplicate node detection.*

I. Introduction

Wireless Sensor Networks(WSNs) are a pervasive technology that targets the connectivity between sensor nodes in multiple environments. Its infrastructure is usually composed of a large number of small autonomous devices called sensor nodes, which runs upon relatively inexpensive computational processes. Sensor nodes harvest information such as temperature, pressure or vibrations etc., from their physical environment and forward sensed values to a set of central points, referred as sink nodes, for appropriate processing. Sensor nodes can sense the environment, communicate with neighbour nodes, and perform basic computations on collected data at the base station. Installation flexibility and easy configuration enable better usability and maintenance than traditional communication technologies.

There are many existing protocols, techniques and concepts from traditional wireless network, such as mobile ad-hoc network, cellular network, wireless local area network and Bluetooth, that are applicable and still used in WSN, but there are lot of fundamental differences which initiate the need of new techniques and protocols. Some of the most important characteristic differences are, in WSNs, number of nodes is much higher than any traditional wireless network. Depending on the application, nodes may be in order of even millions. Thus, it requires an extremely scalable solution to make sure sensor network operations without any interruption. WSNs have large number of sensor nodes due to this addresses are not assigned to them. Instead of address centric, sensor networks are data-centric. Operations of sensor networks are concentrated on data instead of individual sensor node. Thus, sensor nodes need collaborative efforts. Most of traditional wireless networks use point-to-point communications, whereas sensor networks use broadcast communications.

In static wireless sensor network (SWSNs) have gained a great deal of attention in the past decade due to their wide range of application areas and formidable design challenges. In general, wireless sensor networks consist of hundreds and thousands of low-cost, resource-constrained, distributed sensor nodes, which usually scatter in the surveillance area randomly, working without attendance. If the operation environment is hostile, security mechanisms against adversaries should be taken into consideration. Among many physical attacks to sensor networks, the node clone is a serious and dangerous one. Because of production expense limitation, sensor nodes are generally short of tamper-resistance hardware components; thus, an adversary can capture a few nodes, extract code and all secret credentials, and use those materials to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that seem legitimate can freely join the sensor network and then significantly enlarge the adversary's capacities to manipulate the network maliciously.Clones would be authenticated as original nodes in a key establishment scheme of WSNs in different locations, eventually taking over a local segment or an entire network to launch a different types of attacks, such as corrupting data aggregation, injecting false data, and dropping packets selectively. Thus, it is essential to detect clone nodes without delay for minimizing their damages to WSNs.

In this paper to select efficient clone detection schemes such as static versus mobile, centralized versus distributed, random uniform versus grid, whole area versus local area detection.we divide static and mobile sensorsaccording to their mobility. A static sensor node cannot move,while the location of a mobile sensor changes depending onoperational scenarios, all nodes are free to move randomly[6], [10]. The network performance and usefulnessmay depend upon their pre-assembled network settings.schemes to centralized and distributed schemes, i.e., in terms of the ways to collect and verify evidence of clones with help of digital signature. One is that a central node, such as a base station (BS)[4], acts solely on detecting clones, and the other is that a group of sensor nodes conduct the clone detection cooperatively. Furthermore presentaccompanying a new methods of clone detection schemes in wireless sensor network and simulation experiments to compare former clone detection schemes were discussed.

II. Related Work

A. Base station approach

A centralized base station scheme is as a basic clone detection scheme. most probably, each node sends IDs and estimates the locations of its neighbors to a base station(BS). If there is a collision of IDs in far different locations, then the BS revokes the matching sensor nodes by broadcasting an authentic command [4].Also proposedCentral clone detection approaches the key are randomly pre-distributed.If a key is used for several times over a predefined threshold, than the base station revokes the corresponding key as a clone key [5].

B. Randomized multicast approach

The distributed replica detection approach, in which node-to-network broadcast was used. Every node collects the IDs and locations of its neighbors, and it broadcasts them to a network. When a node receives a broadcast message from others, it should be compares the neighbors with its own. If there is a collision of IDs in far different locations, then the BS revokes the matching sensor nodes.

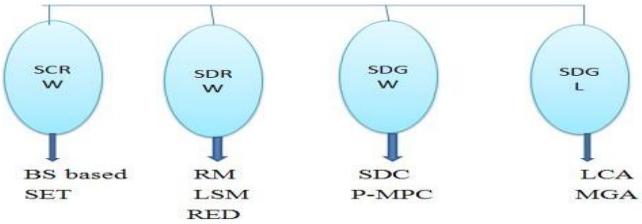


Fig.1. Static sensor node in WSNs

C. Randomized efficient and distributed approach

The randomized, efficient anddistributed (RED) scheme to improve the detection ratio ofRM by increasing the collision probability using a specificpseudo random function. There are several other derivatives or improved version of the line selected multicast (LSM) scheme, such as a distributed hash table based scheme [11], an active detection scheme that works by receiving its neighbors IDs and location from a randomly chosen witness node, a clone detection scheme collecting neighbor instead of locations and finding the duplicate node with in fraction of the seconds.

D. Single deterministic cell approach

Single deterministic cell (SDC) and parallel multiple probabilistic cells (P-MPC), which improve the collision probability of RM by using grid information given to each node. In SDC, the IDs and locations of the neighbors are forwarded to a single zone that is determined from one-wayhash function with a node ID as input. However in P-MPC, the pair information is forwarded to multiple zones that are determined in the same way. Then, every node checks whether or not the IDs received from the other nodes are in contact. Although P-MPC requires a higher communication cost than SDC, it can detect clones by virtue of nodes in the otherzones, even in the case where all nodes in a given zone arecompromised by an opponent.

E. Location claim approach

Location claim approach (LCA) and multi group approach (MGA), to reduce the detection error of the basic approachvia letting the neighbours of an erroneously deployed nodesend out its location to the nodes in the predetermined zonein an authenticated manner. The schemes reduce detectionerrors significantly by checking a collision of ID in two zones.

D. Time Deployment approach

In this new approach all nodes are stored their deployment time. If the packets sent one node to another node the receiver can receive the packet and it should be sent the acknowledgement. If could not receive the acknowledgement can check all nodes deployment times and finding the clone nodes. Which node varying over the threshold time that node must determine the clone nodes.

III. Duplicate Node Detection Schemes

A carbon copy attack means that an opponent injects one or more replicated nodes into a network by using the same ID as another node, i.e., a captured node [3], to negotiation a large portion of a network successfully. With regard to this attack, it is assumed that an opponent captures only a very small portion of nodes in the network because capturing a large portion may not even require clones at all and must be much more costly and easier to detect. It is reasonable to assume that an opponent captures only a small number of nodes and makes clones by replicating the captured nodes to inject them back into the network for achieving adversarial objectives, such as controlling the target area and so forth. Since the opponent already knows the secret of the captured node, it is useless to employ the existing security systems,such as the ones given. Thus, the replica detection is necessarily required and it is compulsory on the following replica detection circumstances. The compromised nodes or the nodes having malicious activity by attacker may not forward or drops the packets.The scheme should also revoke the replicated nodes, so that non faulty nodes in the network cease to communicate with any nodes injected in this fashion.

IV. Mobile Wireless Sensor Newark

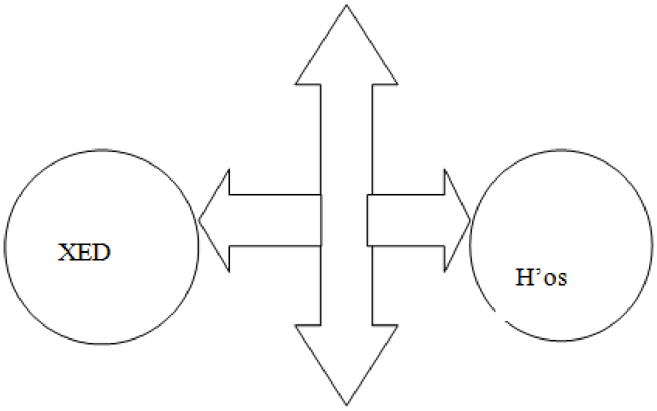
In mobile WSNs is the node moving while the location of a mobile sensor changes depending on operational scenarios. A clone attack means that an adversary injects one or more replicated nodes into a network by using the same ID as another node, i.e., a captured node, to compromise a large fraction of a network successfully. With regard to this attack, it is assumed that an adversary captures only a tiny fraction of nodes in the network because capturing a large fraction may not even require clones at all and must be much more costly and easier to detect. It is reasonable to assume that an adversary captures only a small number of nodes and makes clones by replicating the captured nodes to inject them back into the network for achieving adversarial objectives, such as controlling the target area and so forth. Since the adversary already knows the secret of the captured node, it is useless to employ the existing security systems.

A. Extremely efficient approach

A centralized detection scheme for mobile WSNs by exploiting the fact that a genuine node never moves beyond the maximum speed. Every node in WSNs collects the IDs and locations of its neighbours along with their communication times,3 and every node then transmits the collected data to the BS in an authentic way. If a node moving over the maximum speed is found, then the BS determines that the node is replicated.

In distributed detection scheme, called extremely efficient detection (XED), for mobile WSNs. In XED, mobile nodes exchange their IDs and random numbers when they meet each other, and they record them for further verification. If the previously exchanged random numbers match when the meet again, then they update random numbers

Whole area detection



Local area detection

Fig.2. Mobile sensor node in WSNs

V. Digital Signature

Digital signaturehave always been an internal part of cryptography in history. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of WSNs.Due to the limited battery power, redundant ACK process can degrade the life span of the entire network.

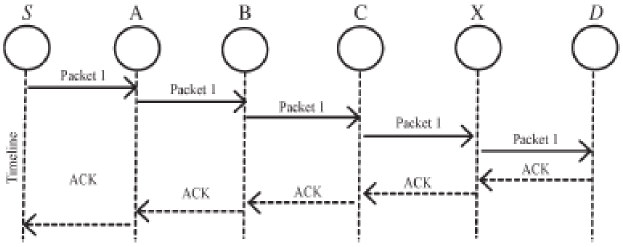


Fig.3. ACK scheme: The destination node is required to sent acknowledgement packets to the source node.

Digital signature schemes can be mainly divided into following two categories.

1) *Digital signature with appendix:*

The original message is required in the signature verification algorithm. For example include a digital signature algorithm(DSA)

2) *Digital Signature with message recovery*:

This type of scheme does not require any other information besides the signature itself in the verification process. For examples implement both DSA and RSA.

A fixed-length message digest is computed through a preagreed hash function H for every message m.

H(m)=d

The sender Alice needs to apply its own private key Pr-Alice on the computed message digest. The result is a signature Sig-Alice.Which is attached to message m and Alice’s secret private key.

Spr-Alice(d)=SigAlice

Alice can send a message m along with the signature SigAlice to Bob via an unsecured channel.

Bob then computes the received message m` against the preagreed hash function H to get the message digest d`. This process can be generalized as

H(m`)=d`

Bob can verify the signature by applying Alice’s public key Pk-Alice on SigAlice ,by using SPk-Alice(SigAlice)=d.

If d=d`,then it is safe to claim that the message m` transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

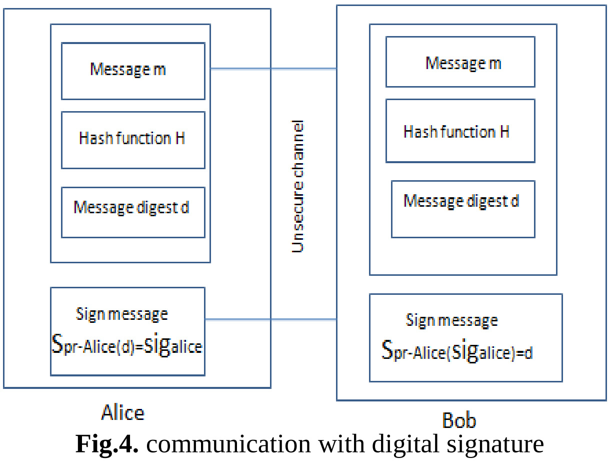


Fig.4. communication with digital signature

VI. Simulation of Duplicate Detection Schemes

Based on the aforementioned selection criteria, we con-ducted the simulation experiments on the representative clone detection schemes with regard to detection performance. For this purpose, we run the simulations in each scenario for a duration of 1000 s using a ns-2 network simulator [22].Each node uses IEEE 802.11 as a media access control protocol,6 in which the transmission range is 100 m, and the sizes of the areas covered by static WSNs and mobile WSNs are 1000 m × 1000 m and 500 m × 500 m, respectively.To test the detection schemes under the same simulation environments as used, focused on detecting single node replications (two clones reproduced from a single genuine node) and then calculated the average of simulation results through more than 150 simulation experiments, which were collected and analysed based on our performance metrics.

Table I: Simulation Parameters

Simulation parameters	Values
Simulation time	1000 s
Field size for static and mobile WSNs	1000m×1000m and 500m×500m, respectively
Velocity of mobile node	1-20 m/s
Radio range	100 m
Initial energy for static and mobile node	10^3 and 10^5 mj, respectively

A given speed between a minimum speed (1 m/s) and a maximum speed (20 m/s), and each mobile node then moves to another randomly chosen location. This random movement process isrepeated throughout the entire simulation period.

A. Static node

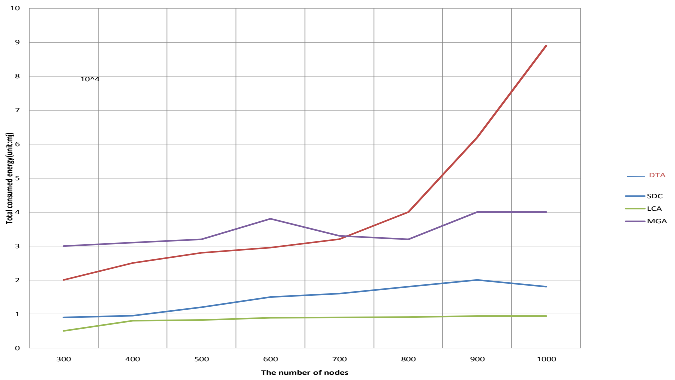


Fig.5. Comparison of energy consumption in static sensor node in WSNs

To compare the clone detection schemes classified by the selection criteria, measure their Ed ,Pd, and Td , and in which the x-axes describe the number of nodes in the network and the y-axes give Ed . Moreover, both values in parentheses give Pdand Td , respective.

B. Mobile node

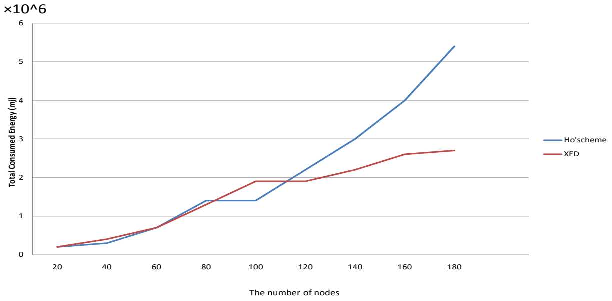


Fig.6. Comparison of energy consumption in mobile node in WSNs

To design a local network detection scheme, however, thereare two essential requirements. The first requirement is the grid deployment. When numerous sensors are deployed, the grid deployment may be more reasonable than the random uniform deployment. As it is difficult to deploy numerous sensors at one time, it is more practical to deploy sensors at several distinct times. A simple way to deploy a series of sensors would be to keep the groups of nodes marked with the group IDs and to use a marked map with the group IDs on it. The group ID can be a zone ID. All it needs is a map of the given field and a way to predetermine the deployment points, such as assigning a point on a grid to each group. This assertion is considerably supported by the fact that the grid deployment strategy has been used for various applications in WSNs, such as key distribution [27], anomaly detection in localization [28], and public key authentication [29]. Moreover, some researchers showed that the grid deployment requires less density of nodes than the random deployment does, for achieving the same level of coverage. The second requirement is to verify the zone IDs received from its neighbors. If the zone IDs are fabricated, then the local detection schemes will be useless.

Table.2. Energy comparison

Sl.No	Replica detection schemes	Energy savings
1	BS (Base station)	50.3%
2	RM (Randomized Multicast)	75.55%
3	LSM (Line Selected Multicast)	75.55%
4	SDC(Single Deterministic Cell)	84.37%
5	P-MPC(Parallel Multiple Probabilistic Cell	84.37%
6	LCA (Location claim Approach)	94.44%
7	TDA(Time Deployment Approach)	98.21%

VII. Conclusion

The simulation results for the clone detection schemes representing different classification criteria are analysed.It is found that the clone deduction along with security based digital signature scheme is efficient in compared with the existing schemes. From the simulation results, it is noted that TDA can save energy by up to 98.21% and 94.4% as compared to LCA and LSM. Such energy savings are highly desirable and often required in many ad hoc sensor network applications, such as monitoring emergency disaster notification data.

References

[1] Kwantae Cho, Minho Jo, “Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks” IEEE systems Journal, vol,7 ,No. 1,march 2013.

[2] 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.

[3] H. Choi, S. Zhu, and T. F. L. Porta, “SET: Detecting node clones in sensor networks,” in Proc. Security Privacy Commun. Netw. Workshops, 2007, pp. 341–350.

[4] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, “Real-time detection VI. Conclusion of clone attacks in wireless sensor networks,” in Proc. ICDCS, 2008, pp. 3–10,

[5] B. Sun, L. Osborne, Yang Xiao and S. Guizani, “Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks,” IEEE Wireless Communications, pp. 56-63, October 2007.[8] 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. 5, pp. 677–691, Jun. 2010.

[6] Z. Li and G. Gong, “Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks,” in *Proc. IEEEInt. Conf. Mobile Adhoc Sensor Syst.*, Oct. 2009, pp. 1030–1035.

[7] 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.

[8] J. W. Ho, D. Liu, M. Wright, and S. K. Das, “Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks,” *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1476–1488, Nov. 2009.

[9] J. W. Ho, M. Wright, and S. K. Das, “Fast detection of replica node attacks in mobile sensor networks using sequential analysis,” in *Proc.IEEE Int. Conf. Comput. Commun.*, Apr. 2009, pp. 1773–1781.

[10] C. M. Yu, C. S. Lu, and S. Y. Kuo, “Mobile sensor network resilient against node replication attacks,” in *Proc. IEEE Commun. Soc. Conf.Sensor Mesh Ad Hoc Commun. Netw.*, Jun. 2008, pp. 597–599.

[11] L. Zhang, Y. Hu, and Q. Wu, “Identity-based threshold broadcast encryption in the standard model,” *KSII Trans. Internet Inform. Syst.*, vol. 4, no. 3, pp. 400–410, Jun. 2010.

[12] A. Mohaisen, J. W. Choi, and D. Hong, “On the insecurity of asymmetric key-based architecture in wireless sensor networks,” *KSIITrans. Internet Inform. Syst.*, vol. 3, no. 4, pp. 376–384, 2009.

[13] T. Shon and Y. Park, “A hybrid adaptive security framework for IEEE 802.15.4-based wireless sensor networks,” *KSII Trans. Internet Inform.Syst.*, vol. 3, no. 6, pp. 597–611, Dec. 2009.

[14] A. Mohaisen, D. Nyang, and T. AbuHmed, “Two-level key pool design-based random key pre-distribution in wireless sensor networks,” *KSII Trans. Internet Inform. Syst.*, vol. 2, no. 5, pp. 222–238, 2008.

[15] M. M. Haque, A. K. Pathan, C. S. Hong, and E. Huh, “An asymmetric key-based security architecture for wireless sensor networks,” *KSIITrans. Internet Inform. Syst.*, vol. 2, no. 5, pp. 265–279, Oct. 2008.

[16] A. Seshadri, M. Luk, and A. Perrig, “SAKE: Software attestation for key establishment in sensor networks,” in *Proc. Distributed Comput.Sensor Syst.*, 2008, pp. 372–385.

[17] P. Zhang and M. Martonosi, “LOCALE: Collaborative localization estimation for sparse mobile sensor networks,” in *Proc. 7th Int. Conf.IPSN*, 2008, pp. 195–206.

[18] Z. Su, F. Shang, and R. Wang, “A wireless sensor network location algorithm based on simulated annealing,” in *Proc. Int. Conf. Biomed.Eng. Inform.*, 2009, pp. 1–5.

[19] M. Kadkhoda, M. Totounchi, M. H. Yaghmaee, and Z. Davarzani, “A probabilistic fuzzy approach for sensor location estimation in wireless sensor networks,” in *Proc. IEEE Int. Conf. Fuzzy Syst.*, Jul. 2010, pp.1–5.

[20] X. Zhou, H. Shi, and W. Shang, “The evaluation method of sensorlocation for transmission fault diagnosis,” in *Proc. IEEE Youth Conf.Inform. Comput. Telecommun.*, Nov. 2010, pp. 190–193.

[21] C. Y. Chow, M. F. Mokbel, and T. He, “A privacy-preserving location monitoring system for wireless sensor networks,” *IEEE Trans. MobileComput.*, vol. 10, no. 1, pp. 94–107, Jan. 2011.

[22] A. Gupta, S. Tapaswi, and V. Jain, “Recurrent grid based voting approach for location estimation in wireless sensor networks symposia and workshops on ubiquitous,” in *Proc. UIC-ATC*, vol. 1. 2009, pp. 333–336.

[23] S. Ganeriwal, C. Popper, S. Capkun, and M. B. Srivastava, “Secure time synchronization in sensor networks,” *ACM Trans. Inform. Syst.Security*, vol. 11, no. 4, p. 23, 2008.

[24] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, “Secure and efficient time synchronization in heterogeneous sensor networks,” *IEEE Trans.Vehic. Technol.*, vol. 57, no. 4, pp. 2387–2394, Jul. 2008.

[25] L. Ma, H. Zhu, G. Nallamothu, B. Ryu, and Z. Zhang, “Impact of linear regression on time synchronization accuracy and energy consumption for wireless sensor networks,” in *Proc. IEEE MILCOM*, Nov. 2008, pp. 1–7.

[26] D. Jiadong, G. Lichen, and Z. Chunxiang, “Research and application on time synchronization of wireless sensor network based on information fusion,” in *Proc. ICCET*, vol. 3. Apr. 2010, pp. V3-75–V3-77.

[27] X. Z. Tian, Y. G. Miao, W. Xu, B. J. Fan, and J. Pan, “Research on time synchronization for wireless sensor networks based on Bayesian estimation Asia-Pacific,” in *Proc. Conf. Wearable Comput. Syst.*, 2010, pp. 155–158.

[28] L. Gheorghe, R. Rughinis, and N. Tapus, “Fault-tolerant flooding time synchronization protocol for wireless sensor networks,” in *Proc. ICNS*, 2010, pp. 143–149.A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, Mar. 2005, pp. 324–328.

[29] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, “Analyzing and modeling encryption overhead for sensor network nodes,” in *Proc. 2nd ACM Int. Conf. Wirel. SensorNetw. Applicat.*, 2003, pp. 151–159.

[30] A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,” in *Proc. IPSN*, Apr. 2008, pp. 245–256.

[31] W. Du, J. Deng, Y. S. Han, S. Chen, and P. Varshney, “A key management scheme for wireless sensor networks using deploymentknowledge,” in *Proc. IEEE Int. Conf. Comput. Commun.*, Mar. 2004, pp. 586–597.