International Journal of Advanced Information in Engineering Technology (IJAIET)

Vol.4, No.9, Sep 2017 ISSN: 2454-6933

Trusted and accurate data transmission on cluster based sensor networks

Sahithi Kuthuru[1], G. Radha Devi[2]
PG Student[1], Assistant Professor[2]
Department of Computer Science and Engineering

Samskruti College of Engineering and Technology

Kondapur, Ghatkesar, Hyderabad

Abstract
Secure information transmission is a basic issue for remote sensor systems (WSNs). Grouping is a powerful and down to earth approach to improve the framework execution of WSNs. In this paper, we consider a safe information transmission for bunch based WSNs (CWSNs), where the groups are framed progressively and intermittently. We propose two Secure and Efficient information Transmission (SET) conventions for CWSNs, called SET-IBS and SET-IBOOS, by utilizing the Identity-Based computerized Signature (IBS) conspire and the Identity-Based Online/Offline advanced Signature (IBOOS) plot, individually. In SET-IBS, security depends on the hardness of the Diffie-Hellman issue in the matching space. SET-IBOOS additionally diminishes the computational overhead for convention security, which is essential for WSNs, while its security depends on the hardness of the discrete logarithm issue. We demonstrate the plausibility of the SET-IBS and SET-IBOOS conventions regarding the security necessities and security examination against different assaults. The counts and recreations are given to show the effectiveness of the proposed conventions. The outcomes demonstrate that, the proposed conventions have preferred execution over the current secure conventions for CWSNs, as far as securityoverhead and vitality utilization.

Index Terms—Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission protocol.

1.Background and Motivations

Group based information transmission in WSNs, has been examined by analysts so as to accomplish the system versatility and administration, which amplifies hub lifetime and decrease data transfer capacity utilization by utilizing neighborhood coordinated effort among sensor hubs [3]. In a group based WSN (CWSN), each bunch has a pioneer sensor hub, viewed as bunch head (CH). A CH totals the information gathered by the leaf hubs (non-CH sensor hubs) in its group, and sends the accumulation to the base station (BS). The LEACH (Low-Energy Adaptive Clustering Hierarchy) convention displayed by Heinzelman et al. [4] is a generally known and viable one to decrease and adjust the aggregate vitality utilization for CWSNs. Keeping in mind the end goal to avoid fast vitality utilization of the arrangement of CHs, LEACH haphazardly turns CHs among all sensor hubs in the system, in rounds. Filter accomplishes changes as far as system lifetime.

Following LEACH, various conventions have been displayed, for example, APTEEN [5] and PEACH [6], which utilize comparative ideas of LEACH. In this paper, for accommodation, we call this kind of bunch based conventions as LEACH-like conventions. Scientists have been generally considering CWSNs in the most recent decade in the writing, be that as it may, the usage of the bunch based engineering in this present reality is somewhat muddled [7]. Adding security to LEACH-like conventions is testing, since they progressively, haphazardly and intermittently modify the system's groups and information joins [8]. In this manner, giving relentless durable hub to-hub trust connections and basic key conveyances are insufficient for LEACH-like conventions (most existing arrangements are accommodated disseminated WSNs, yet not for CWSNs). There are some safe information transmission conventions in view of LEACH-like conventions, for example, SecLEACH [8], GS-LEACH [9] and RLEACH [10]. Mostof them, be that as it may, apply the symmetric key administration for security, which experiences a supposed vagrant hub issue [11]. This issue happens when a hub does not share a pairwise enter with others in its preloaded key ring, so as to moderate the capacity cost of symmetric keys, and the key ring is not adequate for the hub to share pairwise symmetric keys with the majority of the hubs in a system. In such a case, it can't take an interest in any group, and along these lines, needs to choose itself as a CH. Moreover, the vagrant hub issue diminishes the likelihood of a hub joining a CH, when the quantity of alive hubs owning pairwise keys diminishes after a longterm operation of the system. Since the more CHs chosen independent from anyone else, the more general vitality expended of the system [4], the vagrant hub issue builds the overhead of transmission and framework vitality utilization by raising the quantity of CHs. Indeed, even for the situation that a sensor hub shares a pairwise key with a removed CH yet not a close-by CH, it requires relatively high vitality to transmit information to the far off CH.

1.1 Contributions and Organization

As of late, we have connected and assessed the key administration of IBS to steering in CWSNs [17]. In this paper, we expand our past work and concentrate on giving effective secure information correspondence to CWSNs. The commitments of this work are as per the following. We propose two Secure and Efficient information Transmission (SET) conventions for CWSNs, called SET-IBS and SETIBOOS, by utilizing the IBS conspire and the IBOOS plot, separately. The key thought of both SET-IBS and SET-IBOOS is to validate the encoded detected information, by applying advanced marks to message parcels, which are productive in correspondence and applying the key administration for security. In the proposed conventions, mystery keys and matching parameters are disseminated and preloaded in all sensor hubs by the BS at first, which beats the key escrow issue portrayed in ID-based crypto-frameworks [13]. Secure correspondence in SET-IBS depends on the ID-based cryptography, in which, client open keys are their ID data. Subsequently, clients can acquire the comparing private keys without helper information transmission, which is proficient in correspondence and spares vitality. SET-IBOOS is proposed so as to additionally diminish the computational overhead for security utilizing the IBOOS conspire, in which security depends on the hardness of the discrete logarithmic issue. Both SET-IBS and SETIBOOS take care of the vagrant hub issue in the protected information transmission with a symmetric key administration. We demonstrate the attainability of the proposed conventions as for the security prerequisites and investigation against three assault models. Besides, we contrast the proposed conventions and the current secure conventions for productivity by counts and reproductions individually, as for both calculation and correspondence. The rest of this paper is sorted out as takes after. Segment 2 portrays the system design, security vulnerabilities and destinations. Area 3 presents the IBS and IBOOS plans for CWSNs. Segment 4 and 5 show the subtle elements of the proposed SET-IBS and SET-IBOOS, individually, and Section 6 introduces the convention elements and qualities. Segment 7 investigates and assesses the proposed SET-IBS and SETIBOOS. The last segment finishes up this work. 2 System Description and Protocol Objectives This area displays the system engineering, security vulnerabilitiesand convention targets.

2. Network Architecture

Consider a CWSN comprising of a settled base station (BS) and an expansive number of remote sensor hubs, which are homogeneous in functionalities and abilities. We accept that the BS is constantly dependable, i.e., the BS is a put stock in

expert (TA). In the interim, the sensor hubs might be bargained by assailants, and the information transmission might be hindered from assaults on remote channel. In a CWSN, sensor hubs are gathered into bunches, and each group has a bunch head (CH) sensor hub, which is chosen self-rulingly. Leaf (non-CH)n sensor hubs, join a bunch contingent upon the getting signal quality and transmit the detected information to the BS by means of CHs to spare vitality. The CHs perform information combination, and transmit information to the BS specifically with relatively high vitality. Furthermore, we accept that, all sensor hubs and the BS are time synchronized with symmetric radio channels, hubs are appropriated arbitrarily, and their vitality is obliged. In CWSNs, information detecting, preparing and transmission devour vitality of sensor hubs. The cost of information transmission is considerably more costly than that of information handling. Hence, the technique that the middle of the road hub (e.g., a CH) totals information and sends it to the BS is favored, than the strategy that every sensor hub straightforwardly sends information to the BS [1, 3]. A sensor hub switches into rest mode for vitality sparing when it doesn't detect or transmit information, contingent upon the TDMA (time division different get to) control utilized for information transmission. In this paper, the proposed SET-IBS and SET-IBOOS are both intended for similar situations of CWSNs above.

2.1Security Vulnerabilities and Protocol Objectives

The information transmission conventions for WSNs, including clusterbased conventions (LEACH-like conventions), are helpless against various security assaults [2, 21]. Particularly, assaults to CHs in CWSNs could bring about genuine harm to the system, since information transmission and information collection rely upon the CHs on a very basic level. On the off chance that an aggressor figures out how to trade off or put on a show to be a CH, it can incite assaults, for example, sinkhole and specific sending assaults, subsequently disturbing the system. Then again, an aggressor may expect to infuse false detecting information into the WSN, e.g., imagine as a leaf hub sending counterfeit data towards the CHs. All things considered, LEACHlike conventions are more vigorous against insider assaults than different sorts of conventions in WSNs [21]. It is on the grounds that CHs are pivoting from hubs to hubs in the system by rounds, which makes it harder for gatecrashers to recognize the directing components as the middle person hubs and assault them. The attributes in LEACH-like conventions diminish the dangers of being attackedidentify and trade off critical hubs. The objective of the proposed secure information transmission for CWSNs is to ensure a protected and proficient information transmission between leaf hubs and CHs, and also transmission amongst CHs and the BS. Then, the vast majority of existing secure transmission conventions for CWSNs in the writing [8–10], in any case, apply the symmetric key administration for security, which experiences the vagrant hub issue that is presented in Section 1. In this paper, we expect to take care of this vagrant hub issue by utilizing the ID-based crypto-framework that ensures security necessities, and propose SET-IBS by utilizing the IBS conspire. Moreover, SET-IBOOS is proposed to decrease the computational overhead in SET-IBS with the IBOOS plot. In this area, we present the IBS plan and IBOOS conspire utilized as a part of the paper. Note that the regular plans are not particularly intended for CWSNs. We adjust the customary IBS plot for CWSNs by circulating capacities to various types of sensor hubs, in light of [22] at first. With a specific end goal to additionally decrease the computational overhead in the marking and confirmation procedure of the IBS plot, we adjust the regular IBOOS conspire for CWSNs, in view of [23]. In a multiplicative limited cyclic gathering G of prime request q, there exists a component g as the generator and components gx ∈ G,

such that, $G = \_\, g \,\_ = \_gx \mid x \in Z^* \, q\_$,

where, Z^*

$q(Z^* \, q = \{0, 1, \ldots, q-1\})$

is a multiplicative group consisting of $q-1$ integers, in which the multiplication operation in the group ends in the remainder on the division by q (mod q) [24]. The Discrete Logarithm Problem (DLP) [25] in the cyclic group G is to compute x, in which the computational complexity is believed to be hard in this work.

3.The Proposed SET-IBS Protocol

In this paper, we propose two novel Secure and Efficient information Transmission (SET) conventions for CWSNs, called SET-IBS and SET-IBOOS, by utilizing the IBS conspire and the IBOOS plot, separately. We initially display SET-IBS in this area. The proposed SET-IBS has a convention

instatement preceding the system organization and works in rounds amid correspondence, which comprises of a setup stage and a relentless state stage in each round. We present the convention instatement, portray the key administration of the convention by utilizing the IBS plot, and the convention operations a short time later.

3.1 Protocol introduction

In SET-IBS, time is partitioned into progressive time interims as other LEACH-like conventions. We signify time-stamps by Ts for BS-to-hub correspondence and by ti for leaf-to-CH correspondence. Note that key pre-dispersion is an effective strategy to enhance correspondence security, which has been adjusted in WSNs in the writing [8–10, 15–17]. In this paper, we receive ID||ti as client's open key under an IBS plot [22], and propose a novel secure information transmission convention by utilizing IBS particularly for CWSNs (SET-IBS). The comparing private blending parameters are preloaded in the

3.2 Protocol operation

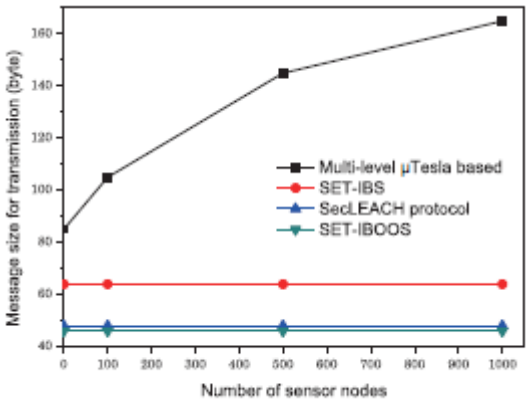
After the convention instatement, SET-IBS works in rounds amid correspondence. Each round comprises of a setup stage and an unfaltering state stage. We assume that, all sensor hubs know the beginning and completion time of each round, on account of the time synchronization. Round Set-up Steady-state Time Frame

Fig. 1. Operation in the proposed secure information transmission

The operation of SET-IBS is isolated by rounds as appeared in Figure 1, which is like other LEACH-like conventions. Each round incorporates a setup stage for building bunches from CHs, and a consistent state stage for transmitting information from sensor hubs to the BS. In each round, the course of events is isolated into back to back schedule openings by the TDMA (time division numerous get to) control [4]. Sensor hubs transmit the detected information to the CHs in each edge of the steadystate stage. For reasonable vitality utilization, hubs are haphazardly chosen as CHs in each round, and other non-CH sensor hubs join groups utilizing one-bounce transmission, contingent upon the most elevated got flag quality of CHs. So as to choose CHs in another round, every sensor hub decides an arbitrary number and contrasts it and an edge. On the off chance that the esteem is not as much as the edge, the sensor hub turns into a CH for the current round. Along these lines, the new CHs are self-chosen based by the sensor hubs themselves just on their nearby choices, in this way, SETIBS capacities without information transmission with each other in the CH revolutions. Table I demonstrates the full strides in one round of SET-IBS. The setup stage comprises of four stages, from Step 1 to 4, and the enduring state stage comprises of the last two stages. In the setup stage, the time-stamp Ts and hub IDs are utilized for the mark era. While, in the enduring state stage, the time-stamp ti is utilized for the mark era securing the

4. Secure Data Transmission with Hierarchical Clustering

In vast scale CWSNs, multi-bounce information transmission is utilized for transmission between the CHs to the BS, where the immediate correspondence is impractical because of the separation or hindrances between them. The rendition of the proposed SET-IBS and SETIBOOS conventions for CWSNs can be expanded utilizing multi-jump directing calculations, to shape secure information transmission conventions for various leveled groups. The answers for this expansion could be accomplished by applying the accompanying two directing models. 1) The multi-jump planar model: A CH hub transmits information to the BS by sending its information to its neighbor hubs, thus the information is sent to the BS. We have proposed a vitality productive steering calculation for progressively bunched WSNs in [30], and it is reasonable for th proposed secure information transmission conventions. 2) The bunch based various leveled technique: The system is broken into grouped layers, and the information bundles go from a lower bunch make a beeline for a higher one, thus to the BS, e.g., [31].



ig. 2. Message size for transmission compared to the number of nodes

4.1 Protocol Evaluation

In this area, we initially present the three assault models of the foes, and give the security investigation of the proposed conventions against these assaults. We at that point introduce comes about acquired from counts and reenactments. We concentrate on the vitality utilization spent on message engendering and calculation. We utilize the system test system OMNeT++ 3.0 to recreate the proposed SET-IBS and SET-IBOOS, and the reproduction source code can be found in [32].

4.2 Security Analysis

So as to assess the security of the proposed conventions, we need to explore the assault models in WSNs which debilitate the proposed conventions, and the situations when an enemy (aggressor) exists in the system. Subsequently, we detail the arrangements and countermeasures of the proposed conventions, against different enemies and assaults.

5 Attack Models

In this paper, we amass assault models into three classes as per their assaulting implies as takes after, and examine how these assaults might be connected to influence the proposed conventions.

• Passive assault on remote channel: Passive aggressors are

ready to perform listening in anytime of the system, or even the entire correspondence of the system. In this way, they can embrace movement investigation or measurable examination in view of the observed or spied messages.

• Active assault on remote channel: Active assailants have

more noteworthy capacity than aloof enemies, which can mess with the remote channels. Along these lines, the aggressors can produce, answer and adjust messages. Particularly in WSNs, different sorts of dynamic assaults can be activated by assailants, for example, false and replayed directing data assault, sinkhole and wormhole assault, specific sending assault, HELLO surge assault, and Sybil assault .

• Node trading off assault: Node bargaining Attackers

are the most capable enemies against the proposed conventions as we considered. The assailants can physically trade off sensor hubs, by which they can get to the mystery data put away in the bargained hubs, e.g., the security keys. The aggressors additionally can change the internal state and conduct of the traded off sensor hub, whose activities possibly fluctuated from the chief convention determinations

6. Answers for Attacks and Adversaries

The proposed SET-IBS and SET-IBOOS give diverse sorts of security administrations to the correspondence for CWSNs, in both setup stage and enduring state stage. Both in SETIBS and SET-IBOOS, the encryption of the message gives privacy, the hash work gives honesty, the nonce and time-stamps give freshness, and the advanced mark gives genuineness and non-renouncement.

• Solutions to aloof assaults on remote channel:

In the proposed SET-IBS and SET-IBOOS, the detected information is encoded by the homomorphic encryption plot from [29], which manages listening stealthily. Accordingly, the inactive foes can't unscramble the listened stealthily message without the decoding key. Moreover, both SET-IBS and SET-IBOOS utilize the key administration of solid ID-based encryption. In light of the DHP presumption said in Section 3, the ID-based key administration in the proposed conventions is IND-ID-CCA secure (semantic secure against a versatile ID-based picked

ciphertext assault) and IND-ID-CPA secure (semantic secure against a versatile ID-based picked plaintext assault). Thus, properties of the proposed secure information transmission for CWSNs settle the countermeasures to uninvolved assaults.

• Solutions to dynamic assaults on remote channel:

Concentrating on the strength against specific assaults to CWSNs said in assault models, SET-IBS and SET-IBOOS function admirably against dynamic assaults. Most sorts of assaults are indicated CHs of going about as middle person hubs, as a result of the constrained capacities by the leaf hubs in a bunch based engineering. Since assailants don't have substantial advanced mark to link with communicate messages for validation, aggressors can't imagine as the BS or CHs to trigger assaults. In this manner, SETIBSm and SET-IBOOS are versatile, and hearty to the sinkhole and particular sending assaults, on the grounds that the CHs being assaulted are skilled to disregard all the correspondence parcels with fake hub IDs or false computerized marks. Together with round-turning system and advanced mark plans, SETIBS and SET-IBOOS are versatile to the welcome surge assaults including CHs.

• Solutions to hub bargaining assaults:

If there should arise an occurrence of assaults from a hub bargaining assailant, the traded off sensor hub can't be trusted any longer to satisfy the security necessities by key administrations. For the situation that the hub has been traded off however works ordinarily, the WSN framework needs an interruption location instrument to identify the bargained hub [33], and needs to supplant the bargained hub physically or relinquish utilizing it. In this part, we explore the impact of the rest of the sensor hubs, and assess the properties just to that piece of the system. Since each round in the convention operations ends in a pre-characterized time, SET-IBS and SET-IBOOS fulfill the property of convention execution end, contingent upon the nearby clock of the sensor hubs. The CH hubs are chosen basedonly on their neighborhood choices, in this manner, both SET-IBS and SET-IBOOS work if there exists a dynamic or trading off aggressor. So as to wipe out the traded off sensor hub in the system, all the repudiated IDs of bargained hubs will be communicated by the BS toward the start of the current round. Along these lines, the traded off hubs can be kept from either choosing as CHs or joining bunches in this round. Besides,

7.1 Simulation Results

Fathoming the additional vitality utilization by the assistant security overhead and delaying the system lifetime are basic in the proposed SET-IBS and SET-IBOOS. With a specific end goal to assess the vitality utilization of the computational overhead for security in correspondence, we consider three measurements for the execution assessment: Network lifetime, framework vitality utilization and the quantity of alive hubs. For the execution assessment, we think about the proposed SET-IBS and SET-IBOOS with LEACH convention and SecLEACH convention.

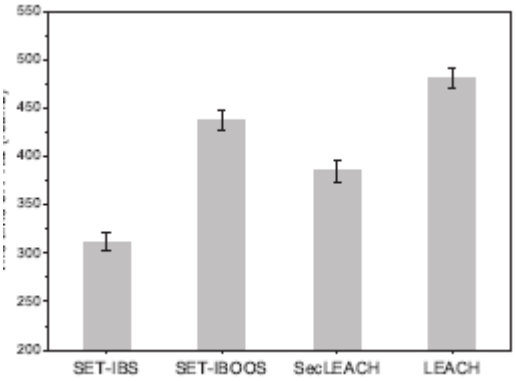
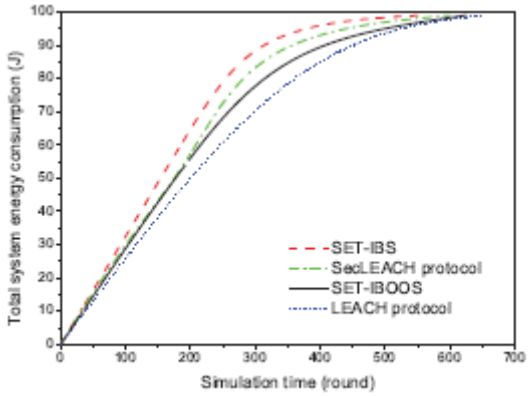


Fig. 3. Comparison of FND time in different protocols



I. Comparison of energy consumption in different protocols

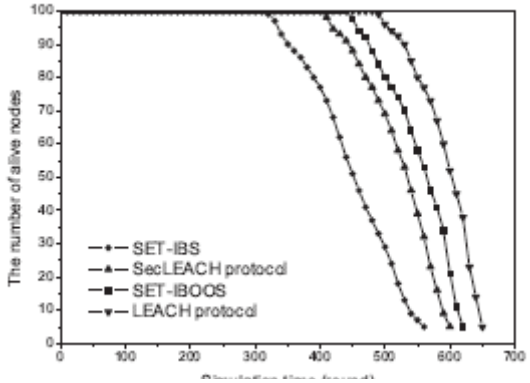


Fig. 5. Comparison of the number of alive nodes in different protocols

• Network lifetime (the season of FND) - We utilize the most general metric in this paper, the season of FND (first hub kicks the bucket), which demonstrates the span that the sensor arrange is completely practical [1]. In this manner, expanding the season of FND in a WSN intends to drag out the system lifetime.

• The quantity of alive hubs –
The capacity of detecting and gathering data in a WSN relies upon the arrangement of alive (hubs that have not fizzled). In this way, we assess the usefulness of the WSN relying upon tallying the quantity of alive hubs in the system.

• Total framework vitality utilization –
It alludes to the measure of vitality devoured in a WSN. We assess the variety of vitality utilization in secure information transmission conventions. In the system reproduction tests, 100 hubs are arbitrarily circulated in a 100m × 100m zone, with a settled BS situated close piece of the zone, as appeared in the figure inm Appendix C.2. All the sensor hubs occasionally sense occasions and transmit the information bundle to the BS. We expect that the sensor CPU is a low-control elite Intel PXA255 processer of 400 MHz, which has been broadly utilized as a part of numerous sensor items, e.g., Crossbow Stargate .

8 Conclusion

In this paper, we initially investigated the information transmission issues and the security issues in CWSNs. The lack of the symmetric key administration for secure information transmission has been talked about. We at that point exhibited two secure and productive information transmission conventions individually for CWSNs, SET-IBS and SET-IBOOS. In the assessment area, we gave attainability of the proposed SET-IBS and SET-IBOOS as for the security necessities and investigation against steering assaults. SET-IBS and SET-IBOOS are proficient in correspondence and applying the ID-based crypto-framework, which accomplishes security necessities in CWSNs, and additionally tackled the vagrant hub issue in the safe transmission conventions with the symmetric key administration. In conclusion, the examination in the count and reproduction comes about demonstrate that, the proposed SET-IBS and SET-IBOOS conventions have preferred execution over existing secure conventions for CWSNs. Regarding both calculation and correspondence costs, we brought up the benefits that, utilizing SET-IBOOS with less assistant security overhead is favored for secure information transmission in CWSNs.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence*, vol. 278. Springer-Verlag, 2010.
[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A

Survey of Security Issues in Wireless Sensor Networks," *IEEE Comm. Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 14/15, pp. 2826-2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Comm.*, vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel & Distributed Systems*, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[7] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int'l J. Computer Applications*, vol. 47, no. 11, pp. 23-28, 2012. [8] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," *Signal Processing*, vol. 87, pp. 2882-2895, 2007. [9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," *Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA)*, pp. 145-152, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," *Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM)*, pp. 1-5, 2008.

[11] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," *Proc. Int'l Conf. Comm., Computing & Security (ICCCS)*, pp. 146-151, 2011. [12] G. Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," *Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom)*, pp. 146-150, 2005.

[13] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proc. Advances in Cryptology (CRYPTO)*, pp. 47-53, 1985.

[15] D.W. Carman, "New Directions in Sensor Network Key Management," *Int'l J. Distributed Sensor Networks*, vol. 1, pp. 3-15, 2005.

[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," *Proc. IEEE Int'l Conf. Computer and Information Technology (CIT)*, pp. 882-889, 2010.

[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," *Proc. IEEE GLOBECOM*, pp. 1-5, 2010. [18] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel & Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[19] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," *Proc. Advances in Cryptology (CRYPTO)*, pp. 263-275, 1990.

[20] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," *Proc. 11th Australasian Conf. Information Security and Privacy*, pp. 99-110, 2006.

[21] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," *Int'l J. Information Security*, vol. 9, no. 4, pp. 287-296, 2010.

[22] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01)*, pp. 213-229, 2001.

[23] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks*, vol. 1, nos. 2/3, pp. 293-315, 2003.

[24] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography (SAC)*, pp. 310-324, 2003.

[25] J.J. Rotman, *An Introduction to the Theory of Groups*, fourth ed. Springer-Verlag, 1994. [26] K.S. McCurley, "The Discrete Logarithm Problem," *Proc. Symp. Applied Math., Programming Computer Science*, vol. 42, pp. 49-74, 1990.

[27] D. Boneh, I. Mironov, and V. Shoup, "A Secure

Signature Scheme from Bilinear Maps," *Proc. RSA Conf. The Cryptographers' Track (CT-RSA)*, pp. 98-110, 2003.

[28] P. Barreto et al., "Efficient Algorithms for Pairing-Based Cryptosystems," *Proc. 22nd Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO)*, pp. 354-369, 2002.

[29] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," *Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous)*, pp. 109-117, 2005.

[30] H. Lu, J. Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks," *Proc. Fourth Int'l Conf. Frontier of Computer Science and Technology (FCST)*, pp. 565-570, 2009.

[31] Y. Jia, L. Zhao, and B. Ma, "A Hierarchical Clustering-Based Routing Protocol for Wireless Sensor Networks Supporting Multiple Data Aggregation Qualities," *IEEE Trans. Parallel & Distributed Systems*, vol. 4, nos. 1/2, pp. 79-91, 2008.

[32] "OMNeT++," *OMNeT++ Community*, http:/www.omnetpp.org/, 2013.

[33] B. Sun et al., "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," *IEEE Wireless Comm. Magazine*, vol. 14, no. 5, pp. 56-63, Oct. 2007.

[34] *Secure Hash Standard*, Nat'l Inst. of Standards and Technology (NIST), Fed. Information Processing Standard Publication, vol. 180, no. 1, 1995.

[35] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[36] D. Liu and P. Ning, "Multilevel μ TESLA: Broadcast Authentication for Distributed Sensor Networks," *ACM Trans. Embedded Computing Systems*, vol. 3, pp. 800-836, 2004.