International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 5; Issue: 6; June-2016

Energy Efficient Scheme for Lifetime Maximization against Power Attack in Wireless Sensor Network

Prof. Anil Kulkarni[1], Prof. Guruprasad Kulkarni[2], Jyothi Jawalge[3]
[1]*Assistant Professor in Department of Computer Science & Engineering, GNDEC, Bidar,*
[2]*Assistant Professor in Department of Computer Science & Engineering, GNDEC, Bidar,*
[3]*M.tech Research scholar in Department of Computer Science & Engineering, GNDEC, Bidar,*
Anilkulkarni51@gmail.com,ankbdr@yahoo.com,jyothi.jawalge@gmail.com

***Abstract*— Security and energy efficiency are the most important concerns in wireless sensor networks (WSNs) design. To save the power and extend the lifetime of WSNs, various media access control (MAC) protocols are proposed. Most traditional security solutions cannot be applied in the WSNs due to the limitation of power supply. The well-known security mechanisms usually awake the sensor nodes before the sensor nodes can execute the security processes. However, the Denial-of-Sleep attacks can exhaust the energy of sensor nodes and shorten the lifetime of WSNs rapidly. Therefore, the existing designs of MAC protocol are insufficient to protect the WSNs from Denial-of-Sleep attack in MAC layer. The practical design is to simplify the authenticating process in order to enhance the performance of the MAC protocol in countering the power exhausting attacks. This paper proposes a cross-layer design of secure scheme integrating the MAC protocol. The analyses show that the proposed scheme can counter the replay attack and forge attack in an energy-efficient way.**

***Keywords*— wireless sensor networks, energy efficiency, denial-of-sleep, power exhausting attacks, secure scheme.**

I. INTRODUCTION

To save energy and extend the lifetime of WSNs, different schemes are researched and proposed [1], [2]. Most of the researchers aim at layer-2 protocol design. In the duty-cycle based WSNs MAC protocols, the sensor nodes are switched between awake/active and sleep state periodically. The sensor nodes are switched into sleep mode after certain idle period [3]-[6]. In the Low Power Listening (LPL) based WSNs MAC protocol, such as B-MAC [3], the receiver wakes up periodically to sense the preamble from the sender and then to receive and process the data. When the sender needs to send data, it sends a long preamble to cover the sleep period to ensure the receiver waking up and sensing. The LPL based MAC protocol is an asynchronous protocol. It decouples the sender and receiver with time synchronization. The X-MAC protocol improves LPL based MAC protocol by replacing the long preamble with shot preambles [6]. Fig. 1 shows the timeline of X-MAC protocol, which allows the receiver to send acknowledgment (ACK) back to the sender as soon as it senses the preamble.

The Denial-of-Sleep is one of the power exhausting attacks of WSNs [7]-[9]. This attack tries to keep the sensor nodes awake to consume more power. In any security mechanism, the sensor nodes must be waked before receiving data and checking security properties. Current layer-2 protocol designsare insufficient to protect a WSN from Denial-of-Sleep attack [7].

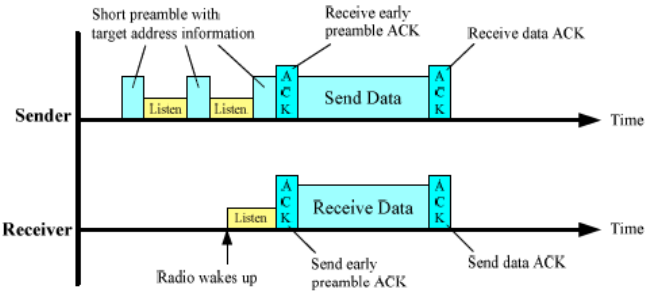


Fig. 1 Timeline of X-MAC protocol

Without security mechanism, an anti-node can broadcast a fake preamble frequently. If the receiver cannot tell the real preamble and the fake one, the receiver will receive and process the data from the anti-node. Such attack will keep the receiver awake as long as the data transmission sustains, which exhausts the battery of nodes rapidly. Moreover, an anti-node can replay a fake preamble ACK to the sender. Thus, the sender will start to send the data to the anti-node but it will never receive the right data ACK. Similarly, the sender may send data repeatedly and exhausts the battery of node rapidly. As a result, the sender and receiver need mutual authentication schemes to counter such attacks.

In traditional wireless security mechanisms, the transmitting data is encrypted with keyed symmetric or asymmetric encryption algorithm. The wireless sensor networks prefer the symmetric algorithm to avoid the complicated computing and heavy energy consumption. But the encrypted data makes the battery exhaustion even worse under Denial-of-Sleep attack. The anti-node can send the encrypted "garbage" data to receiver. This attack forces the receiver to decrypt the data. Before the receiver identifies that the data is "garbage", the receiver consumes more power to receive and decrypt data.

These processes also keep sensor nodes awake longer. An easy and fast mutual authentication scheme is needed to integrate with MAC protocol to counter the encrypted

"garbage" data attack. In this paper, a cross-layer design of secure scheme integrating the MAC protocol, *Two-Tier Energy-Efficient Secure Scheme* (TE_2S), is proposed to protect the WSNs from the above attacks.

The practical design is to simplify the security process when suffering the power exhausting attacks. The design principles and features of the proposed secure scheme are:

1) Energy conservation
2) Low complexity
3) Mutual authentication
4) Symmetric encryption
5) Dynamic session key generated with challenge text
6) Capability to counter the replay attack and forge attack
7) Integrating the MAC protocol

This paper proposes a two-tier secure transmission scheme. This scheme uses the hash-chain to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key. The only computations of dynamic session key are the hash functions, such as MD5 or SHA-1, which are very simple and fast. By integrating with MAC protocol, there is no extra packet compared with the existing MAC designs. The security analysis shows that this scheme can counter the replay attack and forge attack, and the energy analysis shows that this scheme is energy efficient as well.

II. RELATED WORK

In [10]-[12], a dynamic session key policy (DSKP) was proposed based on a one time password (OTP) system to protect users during the authentication process and session key agreement process. The reason for using OTP is that it varies with sessions where the length is long enough compared with a human-chosen password [13]. Therefore, it is hard to trace and detect. By using the counter indicated hash-chain algorithm, the DSKP is computational cheap. But the synchronized counter of hash-chain algorithm may not be suited to the asynchronous LPL based MAC protocol in WSNs. The overhead of security algorithms have been well studied on embedded systems [14]-[16]. Several popular algorithms of symmetric encryption and hashing function were evaluated on varied micro-controller units (MCU) in [15]. Based on experimental tests, the clock cycles and execution time were measured for each algorithm and platform. These analytical models can be derived to indicate the computational cost of given embedded architectures on different encryption schemes.

III. NOTATIONS TO BE USED

In order to facilitate and clarify our presentation the following notations are used in the paper.

ID_X: X's identity.

K_s: session key.

K_c: cluster key.

R_s, R_r: random number selected by sender and receiver respectively.

h(x): a one-way hash function which x is the input.

$E_K(x)$: encrypts x by using symmetric algorithm with key K.

$D_K(x)$: decrypts x by using symmetric algorithm with key K.

$MAC_K(x)$: message authentication function with key K, where x is the input message.

P_{TX}: power of radio in transmit mode.

P_{RX}: power of radio in receive mode.

P_{RI}: power of radio in idle mode.

P_{RS}: power of radio in sleep mode.

P_{AC}: power of MCU in active mode.

P_{MS}: power of MCU in sleep mode.

T_S: duration of node sleep.

T_W: duration of node awake.

T_P: duration of preamble.

T_{PA}: duration of preamble ACK.

T_{PAL}: duration of preamble ACK listening.

T_L: duration of listening in steps.

T_{AC}: duration of MCU active and computing in steps.

T_{TX}: duration of radio transmitting in steps.

T_{RX}: duration of radio receiving in steps.

| : this vertical bar is used to denote concatenation of strings.

IV. THE SECURE TOPOLOGY FORMATION STAGE

In this stage, the secure adaptive topology control algorithm (SATCA) is involved to form the hierarchical topology in four phases: (I) anti-node detection; (II) cluster formation; (III) key distribution; (IV) key renewal [17].

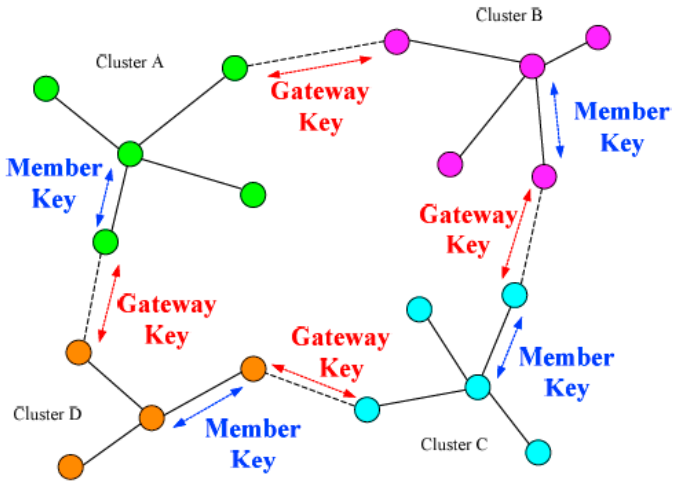


Fig. 2 Key distribution for WSNs

In phase I, an authenticated broadcasting mechanism is applied to identify the anti-nodes. In phase II, the adaptive distributed topology control algorithm (ADTCA) [18] performs the cluster head selection and the gateway selection to form the clusters. In the phase III, two symmetric keys, a cluster key and a gateway key, are distributed locally under cluster construction. The securities of intra- and inter-cluster communication are established upon the cluster key and the gateway key respectively. In phase IV, the key renewing process revokes the old keys and accomplishes the renewal of the keys. The process of key distribution is shown in Fig. 2.

IV. DESIGN PRINCIPLES OF TE2S

After the secure topology formation stage, there is a shared secret key between the valid member nodes and clusterhead of each cluster. A cluster key is a key shared by a cluster head and all its cluster members, which is mainly used for securing local broadcast messages (e.g. routing control information or sensor messages). Based on the secure cluster topology, a two-tier security scheme is performed to transmit information securely and quickly. This scheme can assist the nodes in deciding to switch into sleep mode or to keep awake as soon as possible. In this work, the X-MAC protocol is involved as the basic architecture of the proposed security scheme [6]. The behavior of packet exchange in the X-MAC protocol is shown in Figure 3.

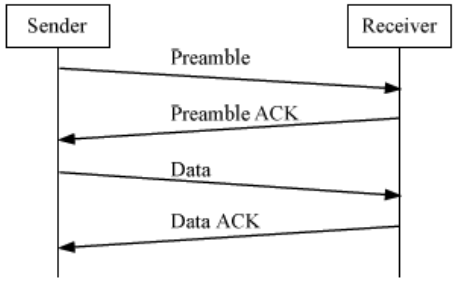


Fig. 3 Packet exchange behaviour in the X-MAC protocol

A. Tier-1: **Session Key Agreement**

In Tier-1, a hash-chain is created by using the cluster key Kc, which is the shared secret between the valid members and the cluster head. This hash-chain is used for mutual authentication and symmetric encryption key. A detailed implementation is described as follows (Fig. 3):

Step 1: The sender selects a random number Rs and computes the secure token (i.e. Token = h(Kc | Rs)).

Step 2: The sender sends its ID, receiver's ID, secure token and random number Rs as the preamble.

Step 3: The receiver verifies the secure token. If the token is not valid, the receiver goes back to sleep mode immediately. If the token is valid, then receiver selects a random number Rr and computes the session key Ks = h(Kc | Rs | Rr). The receiver also computes the hash chain h(Ks) and h(h(Ks)).

Step 4: The receiver sends the h(h(Ks)) and random number Rr as the ACK.

Step 5: The sender computes the session key Ks = h(Kc | Rs | Rr) and the hash chain h(Ks) and h(h(Ks)). The sender then verifies the h(h(Ks)). If the h(h(Ks)) is not valid, the sender will not send the data.

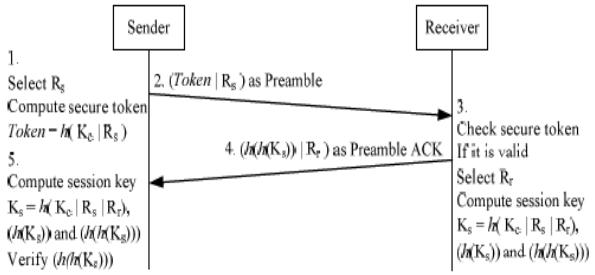


Fig. 4 Session Key Agreement

To check the secure token valid, the receiver executes 1 hash function computing and 1 comparing computing. These 2 computations are very simple and fast. If the secure token is not valid, the receiver goes back to sleep mode immediately and discards all the rest processes. To check the receiver is valid, the sender computes and compares the received h(h(Ks)). If the h(h(Ks)) is not valid, the sender will not send the data. The hash chain h(Ks) and h(h(Ks)) are computed for mutual authentication.

Therefore, the sender and receiver reach a dynamic session key agreement with only one random number selection and three hash function computations respectively. This key agreement does not involve any encryption/decryption computing. The random number is the function of timer to make the operation of the random number generator simple and fast.

B. Tier-2: Data Transmission

With the new created dynamic session key Ks, the sender can encrypt the transmission data via symmetric encryption. A detailed implementation of this process is shown in Fig. 5 and described as follows:

Step 1: The sender sends the h(Ks) and E_SymKs(DATA | MACKs(DATA)) to receiver.

Step 2: The receiver verifies the h(Ks). If the h(Ks) is not valid, the receiver goes back to sleep mode immediately. If the h(Ks) is valid, the receiver decrypts the data and checks the MAC of data.

Step 3: The receiver sends the data ACK to sender.

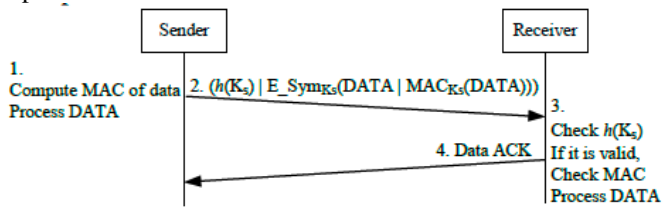


Fig. 5 Data Transmission

Hence, the sender computes h(Ks) from known Ks or Kc. To check the received packet valid, the receiver only compares h(Ks). If the h(Ks) is not valid, the receiver goes back to sleep mode immediately and discards all the rest processes. It is infeasible to compute the h(Ks) from h(h(Ks)). The sender must compute h(Ks) from known Ks or Kc. The hash chain h(Ks) and h(h(Ks) authenticate sender and receiver mutually.

V. IMPLEMENTATION

1. MODULES

a) Duty-cycled WSN creation and routing

In this module, a WSN is created. The sensor nodes and sink in configured and randomly deployed in the network area. The sensor nodes are equipped with energy resource. The sensor nodes are connected with wireless link. The sensor nodes would transmit the data to the Base station nodes. The sensors nodes are assigned with sleep/awake duty cycles over period of time. The sensor nodes need to consume the energy to send, receive the data. The communication is enabled in the network between sensor node and base station

b) Analysis of Power Exhausting in WSN

In this module, the Power Exhausting in the network are analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters.

c) Implementation of SATCA algorithm

In this module, SATCA protocol is implemented. In phase I, an authenticated broadcasting mechanism is applied to identify the anti-nodes. In phase II, the adaptive distributed topology control algorithm (ADTCA) performs the cluster-head selection and the gateway selection to form the clusters. In the phase III, two symmetric keys, a cluster key and a gateway key, are distributed locally under cluster construction. The securities of intra- and inter-cluster communication are established upon the cluster key and the gateway key respectively. In phase IV, the key renewing process revokes the old keys and accomplishes the renewal of the keys.

d) Performance analysis

In this module, the performance of proposed method is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters.

Finally, the results obtained from this module is compared with third module results and comparison X-graphs are plotted. Form the comparison result, final RESULT is concluded.

e) Enhancement Module:

In order to further enhance the security against denial – of – Sleep attacks. In selective authentication process it carries the details of the attacker from previous stage who tries to keep the nodes busy by sending the packets and avoiding them from entering into sleep mode. When source tries to broad cast packets it finds best path and forwards packets to destination. By using bootstrapping technique it also selects three category of nodes as 0,1,2 which acts as firewall , these firewalls identifies the packets (using broadcasting time, if the broadcasting time is less than 0.1 sec, then the node is malicious) send from the attacker and stops the node from flooding packets to destination. This way it avoids sleep attack.

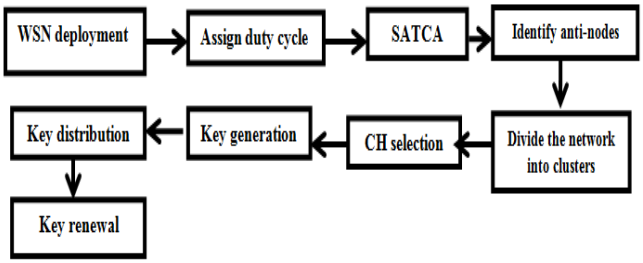
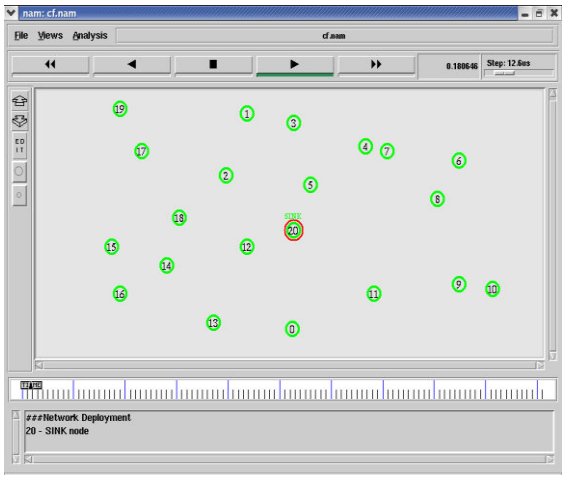


Fig.6 Block diagram for Proposed System

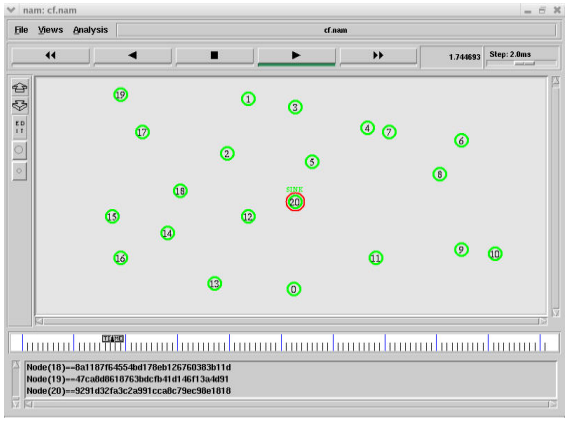
VI. RESULTS

After implementing the proposed system on NS2 platform, the results obtained are as follows:



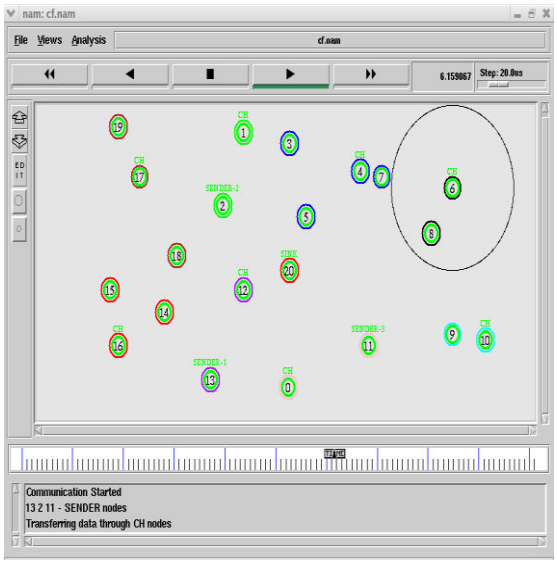
Img. 1 Network Deployment

The network is deplyed with 20 nodes. Here nodes are identified as normal sensor node and SINK node.



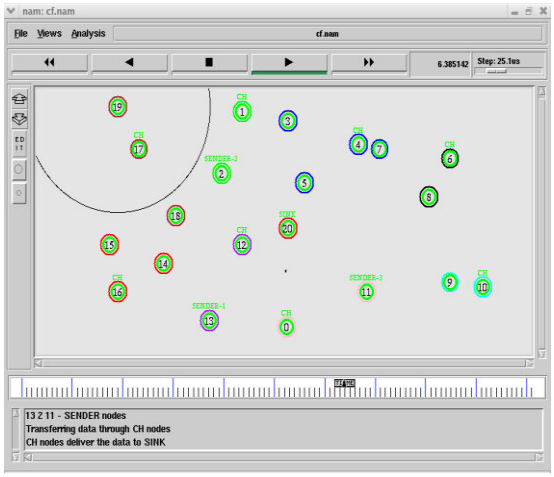
Img. 2 Key Distribution

Here all nodes in the network going to be assigned unique keys.



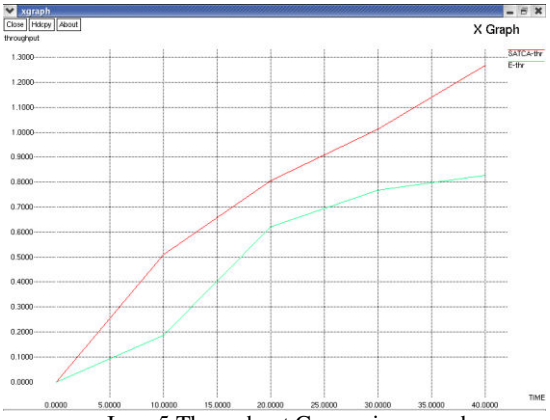
Img. 3 Data Transmission through CH

The network is divided into different clusters, where each cluster is going to have a Cluster Head(CH). CH collect data from its members.



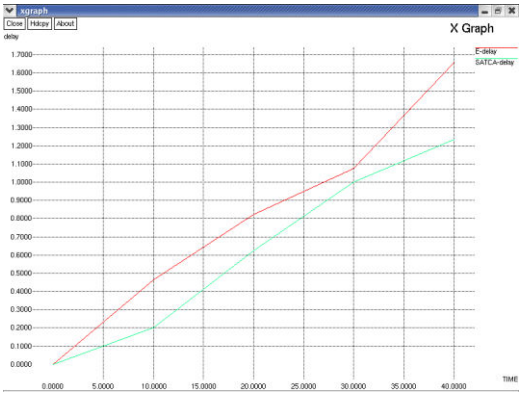
Img. 4 Data transmission from CH to Sink

The CH node after collecting the data from its members, send it to the sink node.



Img. 5 Throughput Comparison graph

The above graph shows the throughput comparison b/w existing system and proposed system. Here propesed system is better(i.e throughput is high) in performance compared to existing system.



Img. 6 Delay Comparison graph

The above graph shows the delay comparison b/w existing system and proposed system. Here propesed system is better(i.e delay is less) in performance compared to existing system.

VII. CONCLUSION

This paper proposes a cross-layer design of energy-efficient secure scheme integrating the MAC protocol. No extra packet is involved in the original MAC protocol design. This scheme can reduce the authenticating process as short as possible to mitigate the effect of the power exhausting attacks. By combination of low complexity security process and multiple check points, the proposed design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible. The security analysis shows that this scheme can counter the replay attack and forge attack. The energy analysis identifies the operating mode precisely, including the MCU and radio modules. The simulation results of normalized energy consumption for normal condition, which has no attacks, show that the proposed scheme increases less than 2.57% in energy consumption of the X-MAC protocol and less than 3.63% in
energy consumption of the RI-MAC protocol with varying packet sending rates. The simulation results of normalized energy consumption for attack conditions also show that the proposed scheme can save times of energy consumptions than X-MAC or RI-MAC does, which also can extend the lifetime of WSNs under attacks. The energy analysis shows that this scheme is efficient in both sender-initiated scheme and receiver-initiated scheme. The overall results show that the proposed secure TE2S scheme can achieve the same throughput performance with less energy consumption. Further energy consumption of the proposed scheme under various duty cycles can be investigated to provide more extensive simulation results to support the efficiency of TE2S scheme in the future.

REFERENCES

[1] G. P. Halkes, T. van Dam, and K. G. Langendoen, “Comparing energysaving MAC protocols for wireless sensor networks,” Mobile Netw.Appl., vol. 10, no. 5, pp. 783–791, 2005.
[2] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, “MAC essentials for wireless sensor networks,” IEEE Commun. Surv. Tuts., vol. 12, no. 2, pp. 222–248, Second Quarter 2010.
[3] J. Kabara and M. Calle, “MAC protocols used by wireless sensor networks and a general method of performance evaluation,” Int. J. Distrib. Sensor Netw., vol. 2012, pp. 1–11, 2012, Art. ID 834784.
[4] M. Li, Z. Li, and A. V. Vasilakos, “A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues,” Proc. IEEE, vol. 101, no. 12, pp. 2538–2557, Dec. 2013.
[5] R. C. Carrano, D. Passos, L. C. S. Magalhaes, and C. V. N. Albuquerque, “Survey and taxonomy of duty cycling mechanisms in wireless sensor networks,” IEEE Commun. Surv. Tuts., vol. 16, no. 1, pp. 181–194, First Quarter 2014.
[6] P. Huang, L. Xiao, S. Soltani, M.W. Mutka, and N. Xi, “The evolution of MAC protocols in wireless sensor networks: A survey,” IEEE Commun. Surv. Tuts., vol. 15, no. 1, pp. 101–120, First Quarter 2013.
[7] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in Proc. 21st Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), Los Angeles, CA, USA, 2002, vol. 3, pp. 1567–1576.
[8] T. van Dam and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks,” in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys), Los Angeles, CA, USA, 2003, pp. 171–180.
[9] J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks,” in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst. (SenSys), Baltimore, MD, USA, 2004, pp. 95–107.
[10] M. Buettner, G. V. Yee, E. Anderson, and R. Han, “X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks,” in
Proc. 4th Int. Conf. Embedded Netw. Sensor Syst. (SenSys), Boulder, CO, USA, 2006, pp. 307–320.
[11] Y. Sun, O. Gurewitz, and D. B. Johnson, “RI-MAC: A receiver-initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in
wireless sensor networks,” in Proc. 6th ACM Conf. Embedded Netw. Sensor Syst. (SenSys), Raleigh, NC, USA, 2008, pp. 1–14.

[12] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop (IAW), New York, NY, USA, Jun. 2005, pp. 356–364.
[13] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in Proc. 7th Int. Workshop Security Protocols, London, U.K., 1999, pp. 172–194.
[14] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 367–380, Jan. 2009.
[15] R. Falk and H.-J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," in Proc. 3rd Int. Conf. Emerg. Security Inf., Syst. Technol. (SECURWARE), Athens, Greece, Jun. 2009, pp. 191–196.
[16] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks," in Proc. 3rd Int. Conf. Ubiquitous Future Netw. (ICUFN), Dalian, China, Jun. 2011, pp. 258–263.
[17] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks," in Proc. 12th Int. Conf. ITS Telecommun. (ITST), Taipei, Taiwan, 2012, pp. 254–258.
[18] V. Srivastava and M. Motani, "Cross-layer design: A survey and the road ahead," IEEE Commun. Mag., vol. 43, no. 12, pp. 112–119, Dec. 2005.
[19] Y.-C. Ouyang, R.-L. Chang, and J.-H. Chiu, "A new security key exchange channel for 802.11 WLANs," in Proc. IEEE 37th Annu. Int. Carnahan Conf. Security Technol. (ICCST), Taipei, Taiwan, Oct. 2003, pp. 216–225.
[20] Y.-C. Ouyang, C.-B. Jang, and H.-T. Chen, "A secure authentication policy for UMTS and WLAN interworking," in Proc. IEEE Int. Conf. Commun. (ICC), Glasgow, U.K., Jun. 2007, pp. 1552–1557.
[21] Y.-C. Ouyang, C.-T. Hsueh, and H.-W. Chen, "Secure authentication policy with evidential signature scheme for WLAN," Security Commun. Netw., vol. 2, no. 3, pp. 259–270, 2009.
[22] N. Haller and C. Metz, A One-Time Password System, document IETF RFC 2289, 1998.
[23] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs, The Security Research Division, Glenwood, WI, USA, Tech. Rep. 00-010, 2000.
[24] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. ACM 2nd ACM Int. Conf. Wireless Sensor Netw. Appl. (WSNA), San Diego, CA, USA, 2003, pp. 151–159.
[25] W. Liu, R. Luo, and H. Yang, "Cryptography overhead evaluation and analysis for wireless sensor networks," in Proc. WRI Int. Conf. Commun. Mobile Comput. (CMC), Kunming, China, Jan. 2009, pp. 496–501.
[26] C.-T. Hsueh, Y.-W. Li, C.-Y. Wen, and Y.-C. Ouyang, "Secure adaptive topology control for wireless ad-hoc sensor networks," Sensors, vol. 10, no. 2, pp. 1251–1278, 2010.
[27] K.-T. Chu, C.-Y. Wen, Y.-C. Ouyang, and W. A. Sethares, "Adaptive distributed topology control for wireless ad-hoc sensor networks," in Proc. Int. Conf. Sensor Technol. Appl. (SensorComm), Valencia, Spain, 2007, pp. 378–386.
[28] A. Perrig, R. Szewczyk, J. D. Tygar, V.Wen, and D. E. Culler, "SPINS: Security protocols for s [29] T. Dimitriou and I. Krontiris, "A localized, distributed protocol for secure information exchange in sensor networks," in Proc. 19th IEEE Int. Parallel Distrib. Process. Symp., Denver, CO, USA, Apr. 2005, p. 240a.
[30] Crossbow MICAz Datasheet, Crossbow Technology Inc., Milpitas, CA, USA, 2006.
[31] Atmel ATmega 128L Datasheet, Atmel Corporation, San Jose, CA, USA, 2009.
[32] Chipcon CC2420 Datasheet, Texas Instruments, Austin, TX, USA, 2007.