A Witness Based Approach to Combat Malicious Packets in Wireless Sensor Network

Usman Tariq[a], Yasir Malik[b], ManPyo Hong[c] and Bessam Abdulrazak[b]
[a]Department of Information Systems, Al-Imam Mohammed Ibn Saud Islamic University, Riyadh, Saudi Arabia
[b]Department of Informatique, University of Sherbrook, Sherbrooke, Quebec, Canada
[c]Graduate School of Information and Communication, Ajou University, Suwon, South Korea

Abstract—*Limitation in resources like processing power, energy and storage capacity has raised security issues for small embedded devices in ubiquitous environments. Moreover, deployment of tiny devices like sensor nodes in these environment, make it easy for intruder to plant attack node or control over the legitimate node for launching the network attack. Such threat raises the issue to design light weight cryptography algorithms to secure such networks. In this paper, we analyzed the basic threat models in wireless sensor network, and proposed a secure witness based approach to combat malicious packets in wireless sensor network. Our model authenticate legitimate broadcast of control packet like HELLO Packet. and identify the adversary communication between nodes. Once the malicious node is identified the localization algorithm can identify the vulnerable node location and can take appropriate actions. Simulation results show the effectiveness of the proposed model.*

Keywords: Sensor networks, encryption, analysis, control packet, authentication, localization

1. Introduction

Recently wireless sensor networks (WSN) and its applications got tremendous attention in industry and research community. A WSN is a Ťself-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world [1] The density of sensor network varies from ten to thousands of sensor nodes depending on the application and network requirement. The deployments can vary from global scale for environmental monitoring, habitat to study emergent environments for search and rescue, in factories for condition based maintenance, in buildings for infrastructure health monitoring, in homes to realize smart homes, or even in bodies for patient monitoring.

Sensor nodes are usually less resourceful in term of energy and computational capabilities, therefore the protocols and application in sensor networks should be designed considering these constraints. In addition to functions, procedures and algorithms which involve various OSI layers two most important elements which can affect the performance of WSN includes security and location determination. Both functions are vital to proper functioning of WSN; without security, data readings can be compromised; without location determination, data readings cannot be spatially associated. The limitation presented by WSN makes them vulnerable and easy to be attacked. In IEEE 802.15.4 standard[1], sensor nodes are requiring to broadcast HELLO packet to inform their presence to their neighboring nodes. The node which receive HELLO packet may assume that the sender is within its communication radius and can respond to the query. Failure to receiving the HELLO packet after a timeout indicates that either the node is no longer a neighbor or it is no longer available. An adversary with high communication radius for example laptop can make this assumption false by broadcasting high transmission routing information to all or a part of the network or by sending false data which would be important for application for decision making.

This paper focused on spoofed HELLO flooding attacks and data authentication and accusation location identification of nodes. We intended to guarantee the secure and smooth communication i.e. (every legitimate network node should receive relevant and updated packet) and defending adversary nodes inside and outside the network. To do so our scheme will identify the malicious node behavior and its location and later appropriate actions can be taken according to network policy.

This paper is organized as followed, In section 2 we summarize the state of art, section 3 presents proposed witness based control packet authentication scheme, in section 4, we shows the performance of and results. Finally, we conclude the paper in section 5..

2. Related Work

Deployments of large number of energy decisive sensor nodes, which will resourcefully enable the information sharing among each other via sharing control and data packets, are defenseless to many kind of routing attacks like HELLO flood. In [1] authors illustrated that every packet delivered by the node is encrypted with a private key and any two sensors share the same common secret. Each time the communication is established between to sensors, algorithm will create a unique key on the fly. It was assumed

[1]IEEE 802.15.4 Standard www.ieee802.org/15/pub/TG4.html

that only reachable neighbor node with decryption key can communicate, which can prevent the adversary attack. The disadvantage of proposed scheme is that any attacker can spoof identities i.e. using HELLO packet, and can begin Sybil attack.

In [4] authors proposed that HELLO flood attack can be prevented using identity verification protocol. Anticipated scheme verifies the bi-directionality of communication signal between two links. If an attack node has a very over the bound link quality, the base station can examine the irregularity by verifying number of trusted neighbors of each node. Approximately all sensing nodes flood the traffic towards base station, which created congestion near centralized sink. In [5] authors recommended that link layer confidentiality and authentication, multi-path routing, and bidirectional link validation can guard sensor nodes from HELLO flood attacks. Considering resource constraint (in processing, communication, energy) of WSN devices, extensively used encryption models and security features used by standard network are not appropriate in WSN. TESLA [8] considers that base station is trusted entity and should be used for distribution the keys between nodes. Receiving nodes has to buffer the packets, which may direct to denial of service (DoS) attack. Furthermore, harmonization is expensive in terms of public key operations. Before transmission starts, sending node has to synchronize with all receivers, which raises the scalability issues. LEAP [13] used dynamic network portioning, which build extra overhead on energy constraint devices. More over, in case of heterogeneous receiving nodes, proposed algorithm has to use many keys with different discloser delays. SeRLoc [6] utilized a distributed range free localization algorithm and it does not restrict any communication among neighboring sensor nodes. SeRLoc protect well against WSN routing threats such as Hello flood, Sybil attack and wormhole attack.

3. Proposed Idea

The motivation of our work is to guarantee the secure routing along with smooth communication i.e. every legitimate network node should receive relevant, updated and accurate packet. Communication paradigm halt if tiny sensor nodes are unavailable due to reasons like spoof hello packet, wormhole attack on control packet and Sybil attack. We categories the attacks as:

Reactive Information Assembly: Cleartext communication between sensor nodes and between sensor node and base station is easily accessible and readable by powerful receiver and well designed antenna holder adversary. This may give liberty to attacker to view the network topology [9].

Node Capture: Attacker can capture and compromise the sensor node. Occupied sensor device may hinder secret data, which adversary can fetch for further use or it can alter the sensor node with updated malicious code, which force node to act abnormal during internodes communication.

False Node: Attacker can add false node to the network, which may broadcast the false information or can deliver the local sensed information to the adversary.

3.1 Witness Based Control Packet Broadcast Authentication

Upon deployment sensor nodes broadcast hello packet to their neighboring nodes to establish link among each other. SNŠs continue hello packet broadcasting on periodical bases, as sensors is energy constrained devices which are deployed in unattended hostile environments [forest, war field, etc], may die because of damage or power failure.

Problem Statement: A laptop class adversary can falsify this postulation by broadcasting control packet (for example, hello packet) with large enough transmission power which can prove to any node in the network that the sender is its neighbor. In sensor network, a hello flood attack uses a single hop broadcast to transmit a message to large number of receivers. An adversary does not always need to be able to construct legitimate traffic in order to use hello flood attack. It can simply rebroadcast overheard by every node in the network. False hello packet may force sensor nodes to forward their packets towards week or possibly dead links.

Solution: The notion of witness requires view of witness when interacting with honest approver to be independent of witness used by prover. Even though witness yields weaker security but in several cases witness indistinguishability is sufficient for specific verification task in hand. Hello packet only satisfies the property of one hope communication, just to get knowledge of nodeŠs neighbors to establish neighboring table and routing path towards base station. In our scenario, after establishing network, if any set of sensor nodes (SA) receives a hello verification request, instead of reply the to SA, forward the Hello request packet to farthest set of nodes which do not lie in the communication range of sender. If î number of nodes verifies the packet receipt from a unique node ID than consider the Hello packet request as false spoofed request and ignore the request. If adversary continuously use the same spoofed node ID for sending high signal false hello packet, than periodically selected secure nodes will vote to base station to block the malicious node ID.

Sensors are tiny reprogrammable device. Any previously authenticated node may become malicious and start misbehaving by sending rapidly generated hello broadcast packet with in its limited communication radius[7]. We maintain a hash table in sensor node.s database, which keeps record of information of control packet sent by certain node ID. For some time duration, if neighboring nodes get hello packets more than predefined threshold than it will report this abnormal behavior to the base station.

Consider a case when adversary using multiple spoofed ID.s send false control packet to base station stating the misbehaving activity of unique/ multiple nodes. Our scheme

effectively encounters this problem by verifying the encrypted header of packet at base station, as each node share a secret key with base station. Further more, because

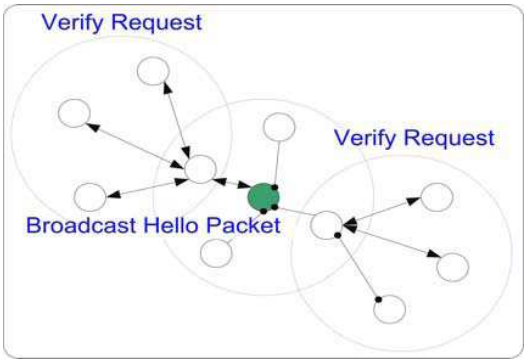


Fig. 1: Broadcast Packet Authentication.

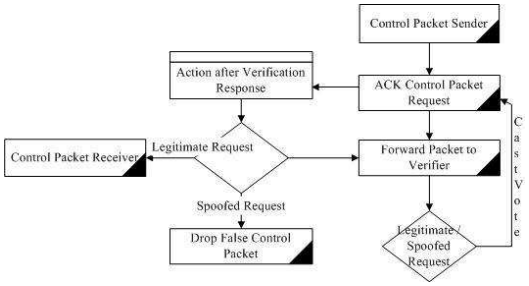


Fig. 2: Broadcast Authentication Procedure.

multiple neighboring nodes will encounter any abnormal activity, and most of them will chose to report to base station because of their homogeneity nature. At base station we also compare the reporting nodes ID.s with the neighboring table of identified possible malicious node. If we found most of reporting nodes do not know reside In side the communication radius of reported node, than we will simply ignore the black listing the particular node request. Consider a case when adversary using multiple spoofed ID.s send false control packet to base station stating the misbehaving activity of unique/ multiple nodes. Our scheme effectively encounters this problem by verifying the encrypted header of packet at base station, as each node share a secret key with base station. Further more, because multiple neighboring nodes will encounter any abnormal activity, and most of them will chose to report to base station because of their homogeneity nature. At base station we also compare the reporting nodes ID.s with the neighboring table of identified possible malicious node. If we found most of reporting nodes do not know reside In side the communication radius of reported node, than we will simply ignore the black listing the particular node request.

Lets consider a scenario where an adversary is generating the false hello flood using several spoofed ID.s. Upon successful hello packet verification, receiving node add senders ID in its neighboring table of tiny database. Most of protocol restricts neighboring table length to some threshold. By using our proposed method, not only we avoid adversary.s hello broad cast attack but also we hinder the buffer overflow attack on neighboring table and routing table

3.2 Data Authentication

Data authentication is a key ingredient of WSN and it plays a vital role in different control processes in network administration for example controlling sensor node duty cycle[3]. Adversary can deploy false nodes in sensor fields and send BS false data which may be essential for decision making process. In this case, during two party communications, data authentication is necessary.

A good cipher should have good randomness, high period; linear span and security against know attacks. We used identity based encryption (IBE), because even in the case of clear text communication, the node must have to learn some basic information before it can communicate with other node. It would be a paradigm shift if the basic information can replace the need of encryption. For example, node M can send message to any near node, with out knowing about its public key (PK). In IBE framework, encryption is always possible. Practically, if receiving node of message does not aware of its private decryption key, it will not be able to decrypt receiving message. However, it will give a strong motivation to node to inquire about the required key. As security point of view, the system can not fully relay on the use of specific information other than PK. As a result, private key computation should be based on global trapdoor information, common to a set of nodes, based on quad zones. This implies, owner of trapdoor (i.e. possibly a key generation center (KGC)), holds the authority to compute the private keys of all sensor field. KGC keep the copies of all keys it generates or has the ability to re-compute the keys of any time stamp and decrypt the communication that it eavesdrops. In other words, KGC can act as key escrow and with additional functionality may behave as IDS watchdog. We can now construct KGC scheme as given under:

Setup: KGC runs *RegPairKeyGenerate*, and generate a PK and the related private key. PK is issued as part of system parameters *pmk*. The private key becomes the KGC.s main key *smk*.

Key Generation: Nodes performs following steps to get their IBE private key:

- Node execute *RegPairKeyGenerate* and generates *pmk* and related *suk* key.
- Node transmits its identity string ID and PK *puk* to KGC. For optimum security, KGC require a verification of awareness of private key *suk*.

- After user.s identity verification, KGC forms a message, "the PK puk is signing key of node ID" and signs it with private key *smk* using *RegSgn*. The resulting output (Cert) is returned to node.

Algorithm 1 Generating a Key

1: *Encryption Model* $(x, \pi_s, \pi_p, (K^1, ..., K^{Nr+1}))$
2: $w^0 \leftarrow x$
3: *for* $w^r \leftarrow (v^r_{\pi p(1)}, ..., v^r_{\pi p(lm)})$ $r \leftarrow 1$ *to* $Nr-1$
4: $u^r \leftarrow w^{r-1} \oplus K^r$
5: *for* $i \leftarrow 1$ *to* m
6: *Do* {
7: *do* $v^r_{(i)} \leftarrow \pi_s(u^r_{(i)})$
8: $w^r \leftarrow (v^r_{\pi p(1)}, ..., v^r_{\pi p(lm)})$
9: $u^{Nr} \leftarrow w^{Nr-1} \oplus K^{Nr}$
10: *for* $i \leftarrow 1$ *to* m
11: *do* $v^{Nr}_{(i)} \leftarrow \pi_s(u^{Nr}_i)$
12: $y \leftarrow v^{Nr} \oplus K^{Nr+1}$ }
13: *Output* (y)

Here, u^r is the input to the S-boxes in random r.u^{r+1} v^r is the output of the S-boxes in round r.W^r is obtained from v^r by applying permutation $\prod_p$, and than u^{r+1} is connected from v^r by x-or-ing the round key k^{r+1}, which is a round key mixing. In the last round, the $\prod_p$ permutation is applied. Signature(s): Nodes are now able to sign messages by using generated certificate Cert. Signing node executes *RegSig* on message *Meg* to be signed, using suk as signing key.

$$\partial = (puk, ncert, s) produceIDbasedsignature \quad (1)$$

To verify generated signature, execute RegVer with PK pmk on ucert and the message Şthe PK puk is signing key of node IDŤ. Verifying node executes RegVer with PK puk on signature and message. If verification return void, the output "*false*" Other wise return "*true*".
Key Distribution: After establishing the link key through multi paths, we used multi path key enforcement method to enhance the security among nodes. This technique is very resilient against node capture attack. The only draw back to adopt such technique is network communication overhead [2]. Nodes discover different paths to route data by exchanging hello packets between them. The more routes discover between two nodes, the more security multi path key reinforcement provides between each link.

3.2.1 Location Information Processing

Research community did splendid tasks to accurately precise location of any node resided in the sensor field. The finite objective of localization algorithm is to gather measurements or related angels between one or many nodes and multiple anchors in order to estimate accurate location estimation. When a node achieves its position evaluation, it may work as new anchor and help neighboring nodes to estimate their position. In our scheme, we focused on non centralized algorithm which distributes the computational load fairly athwart the network nodes, helping all nodes to save computational power available to all network. We did not use signal measurement to infer range. For better understanding, consider a node of interest x resided near Z anchor nodes with harmonizes (an,bn), where n = (1,...,Z). The anchor nodes commune and spread their coordinate points to node of interest. Upon receiving the anchor location information, the node of interest guesstimates its location as the barycenter of given points. The coordinates are estimated as followed:

$$(\hat{a}, \hat{b}) = \left(\frac{1}{z} \sum_{n=1}^{z} a_n, \frac{1}{N} \sum_{n=1}^{z} b_n \right) \quad (2)$$

The barycenter algorithm [12] is localized, disseminated scheme, in which a node of interest needs to be in the neighborhood of *Z* anchor nodes. Note that barycenter algorithm is applicable for single and multi hop setups, but the accuracy of the location estimation will be minimized as the reach ability radii of sensor field nodes increases.

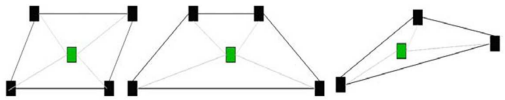


Fig. 3: Multiple scenarios of location estimation using Barycenter Algorithm.

4. Simulation Environment

To verify the effectiveness of our proposed scheme we have simulated our scheme in NS-2[2]. We have assumed identical sensors sensitivities where coverage depends only on geometrical distances from sensors also we have a centralized control server where nodes are connected with each other in peer-to-peer fashion which leads to connectivity with base station. The distance measurement range of the nodes is equal to the communication range. Each node is aware of its two hope neighboring node all the time to avoid data from adversary. Table.1 shows the list of parameters we adopted: Figure 3 illustrates that he amount of computational energy consumed by a security function (cryptography) on a given microprocessor is primarily determined by the processor power consumption, the processor clock frequency, and the number of clocks needed by the processor to compute the security function. The cryptographic algorithm and the efficiency of the software implementation determine the number of clocks necessary to perform the security function.

[2]http://www.isi.edu/nsnam/ns/

Table 1: Simulation Parameters.

Parameter		Values
Area size of simulation		370m * 60m
Total number of nodes in simulation		550
Total time for simulation		100s
Nodes transmission range		15m
Packet or frame error rate		Relative delivery rate
Data rate		Decided by graph
Data Packet Size		70 Bytes
Traffic type		Constant bit rate
RREQ packet Size		36
RREP packet size		40
Inter-Packet transmission delay		Decided by the graph
Beacon Time period		4 sec.
Energy Consumption	Idle	5µJoules/s
	Sense	300Joules
	Transmit	203Joules
	Receive	212 Jouls
Battery Size		0.06 mAH

For cryptographic processing, we assume that energy consumption cannot be significantly reduced via a reduction in clock frequency, since a corresponding reduction in voltage would be required; a capability not ideally available in todayŠs embedded processors.

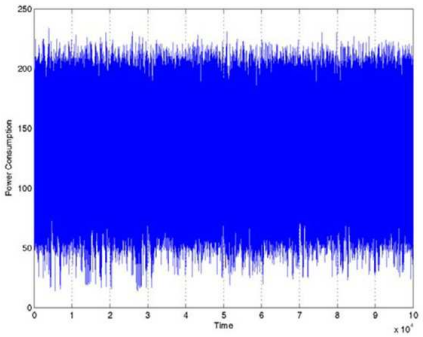
$$LEE = \frac{EncounteredInaccuracyDuringAttack}{HabitualInaccuracu} X100 \quad (3)$$

Figure 4 shows the impact of reach ability radius relative to coverage radius. Its clear that position estimation accuracy improved with node density, for example, for 550 nodes in the sensor field location error is smaller then the case of 100 nodes. Accurate location awareness at quad and whole sensor field can help prevent selfish behavior, Sybil and wormhole (tunneling the broadcast control packets) attacks. Figure 5 demonstrates the association between location error estimation (*LEE*) and the *R* factor while the intensity of malicious nodes generation wormholes is equivalent to 25% of the entire set of sensor nodes in sensor field. The figure illustrates that wormholes influence localization outcome of proposed scheme; where R varies from 5m to 12 m. Since when R = 5 and 12m, the outcome of localization accuracy, which also perform as the denominator in the equation of LEE is not as excellent as when 5 = 5-12m, so it influence that the defection of wormhole, which is calculated with LEE, is not as large as when r = 3, 11m.

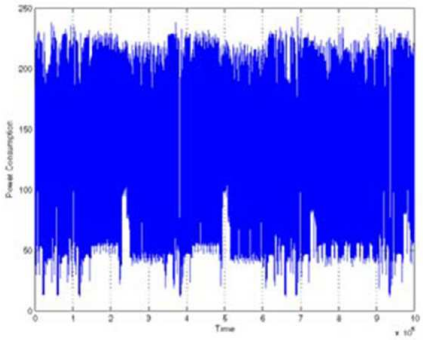
We used radius of signal which has its center at the mean and enclose half of the insight of random vector coordinate evaluation. ^{d} is the measure of ambiguity in position estimation relative to its mean M^{d}. If position estimator is impartial,position error probability (PEP) is a quantifier of the estimator ambiguity relative to accurate node of interest position. If degree of vector is bounded by O, than the probability of 1/2, a particular estimate is with in a distance of O + PEP from the exact position.

$$\frac{1}{2} = \iint_x P\hat{d}(\zeta) d\zeta_1 d\zeta_2 \quad (4)$$

Here $P\hat{d}(\zeta)$is a probability density function of vector estimator $\hat{d}$ and the incorporation area is defined as $x = \left\{\zeta :| \zeta - M\left\{\hat{d}\right\} |\right\} \leq PEP$ where ζ is the distance between the estimated location and actual location. Errors are larger for sparse network densities.



(a) Series a



(b) Series b

Fig. 4: Energy consumption in key distribution.(a) With constant frequency (b) With variable frequency.

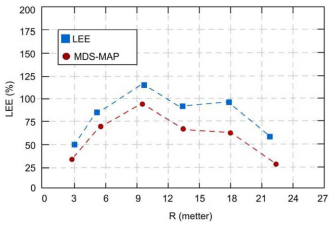


Fig. 5: Effect of number of nodes on Location Estimation Error

From figure 5 we can predict that in the presence of few attack nodes, the localization error may increase drastically. To minimize the localization estimation error percentage encountered because of wormhole we merge wormhole detection and defense mechanism into the localization scheme. The energy reduction achieved via our scheme in contrast to the standard packet with source/destination MAC addresses. To collect a packet, we suppose that the working out takes

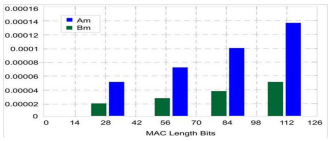


Fig. 6: Total Energy Consumption

on typical 55 commands and additional calculations such as deciphering consumes additional 34 commands, for an overall cost of 12 nJ; packets are 56 bits in size. Energy consumption grows as the packet size expands. Nevertheless, because of the diminutive calculation cost of 1.2 nJ per instruction, the outlay only augments by 5.5 nJ, considering four extra instructions/byte. This implies, in proposed method, the packet requirements to rise only an additional 12.1 kb prior to calculation rate holds the similarity with the rate of broadcasting MAC addresses.

5. Conclusion

In this paper we have presented a simple but efficient mechanism which presents the collateral damage effect caused by control packet flood and clear text communication among nodes. To launch a packet flood an adversary does not always need to be able to construct legitimate traffic in order to use packet flood attack. It can simply rebroadcast overhead by every node in the network.

Proposed IBE encryption model portray, good randomness, high period; linear span and security against know attacks. We believe that it would be paradigm shift if the basic information can replace the need of encryption. This technique is very resilient against node capture attack. The only draw back to adopt such technique is network communication overhead but the more routes discover between two nodes, the more security multi path key reinforcement provides between each link.

In our proposed location information processing scheme, we focused on non centralized algorithm which distributes the computational load fairly athwart the network nodes, helping all nodes to save computational power available to all network. Note that proposed algorithm is applicable for single and multi hop setups, but the accuracy of the location estimation will be minimized as the reach ability radii of sensor field nodes increases. Overall, simulation results show the valuable feasibility of our broadcast control packet authentication, and encryption scheme for embedded architectures. We observed less energy consumption, longer life of network, and better packet authentication.Due to versatile nature of WSN, where authentication and location aware processes come into play, it is and will be an important research field. In future, we have planned to evaluate our encryption scheme to be compared with other scheme like SEAL 3.0 [10] and TEA [11], in terms of software implementation, processing and energy consumption. We look forward for more information on the strengths of the algorithm.

References

[1] S. H. A Hamid, “Defense against lap-top class attacker in wireless sensor network,” in *Advanced Communication Technology, ICACT 2006. The 8th International Conference*, vol. 1, 2006.

[2] R. Anderson, H. Chan, and A. Perrig, “Key infection: smart trust for smart dust,” in *Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on*, oct. 2004, pp. 206 – 215.

[3] C. Boyd and A. Mathuria, “Key establishment protocols for secure mobile communications: A selective survey,” in *Information Security and Privacy*, ser. Lecture Notes in Computer Science, C. Boyd and E. Dawson, Eds. Springer Berlin / Heidelberg, 1998, vol. 1438, pp. 344–355, 10.1007/BFb0053746. [Online]. Available: http://dx.doi.org/10.1007/BFb0053746

[4] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, “Security in wireless sensor networks,” vol. 8, no. 1, 2008, pp. 1–24.

[5] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” in *In First IEEE International Workshop on Sensor Network Protocols and Applications*, 2002, pp. 113–127.

[6] L. Lazos and R. Poovendran, “Serloc: secure range-independent localization for wireless sensor networks,” in *Proceedings of the 3rd ACM workshop on Wireless security*, ser. WiSe ’04. New York, NY, USA: ACM, 2004, pp. 21–30. [Online]. Available: http://doi.acm.org/10.1145/1023646.1023650

[7] S. Lindsey and C. Raghavendra, “Pegasis: Power-efficient gathering in sensor information systems,” in *Aerospace Conference Proceedings, 2002. IEEE*, vol. 3, 2002, pp. 3–1125 – 3–1130 vol.3.

[8] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “The tesla broadcast authentication protocol,” 2002.

[9] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Commun. ACM*, vol. 47, pp. 53–57, June 2004. [Online]. Available: http://doi.acm.org/10.1145/990680.990707

[10] P. Rogaway and D. Coppersmith, “A software-optimized encryption algorithm,” *JOURNAL OF CRYPTOLOGY*, 1997.

[11] D. J. Wheeler and R. M. Needham, “Tea, a tiny encryption algorithm,” in *Fast Software Encryption*, 1994, pp. 363–366.

[12] S.-S. Yu, J.-R. Liou, and W.-C. Chen, “Computational similarity based on chromatic barycenter algorithm,” *Consumer Electronics, IEEE Transactions on*, vol. 42, no. 2, pp. 216 –220, may 1996.

[13] S. Zhu, S. Setia, and S. Jajodia, “Leap: efficient security mechanisms for large-scale distributed sensor networks,” in *Proceedings of the 10th ACM conference on Computer and communications security*, ser. CCS ’03. New York, NY, USA: ACM, 2003, pp. 62–72. [Online]. Available: http://doi.acm.org/10.1145/948109.948120