Energy-Aware Security Management Utilizing Adaptive Security Mechanisms for Wireless Sensor Networks

Mikael Fernandus Simalango
Graduate School of Information and Communication
Department of Computer Engineering Ajou University, South Korea
Email: mikael@ajou.ac.kr

Abstract-*Wireless sensor network is identical with low-power thus communication establishment must consider energy constraint. As a consequence, secure data dissemination over sensor networks is a difficult challenge, considering that establishing secure link and transmitting secure data requires additional resources which may give shortage to network lifetime. This paper offers an alternative to secure data dissemination by adaptively adjusting security policy through reflection of historical data and energy level.*

Keywords: wireless sensor networks, secure communication, adaptive security

I. INTRODUCTION

Wireless sensor networks are becoming more widely adopted and implemented to manage data acquisition and communication among various sensor nodes in a wirelessly-connected area, especially in harsh environment. Wireless sensor networks, however, have different characteristics with other wireless networks such as wireless infrastructure, ad hoc, or cellular networks. This kind of network is associated with low and limited power and minimum supervision. These characteristics, therefore, allude self-regulating and self-maintaining multi-hop networks.

Although supervision in wireless sensor networks can be made possible, for example wireless sensor networks spreading over a city like CitySense [1], it is important to notice that sometimes supervision should be minimized especially when supervision can lead to threat to human safety. The volcano monitoring system [2] shows clear example for this statement.

Although each node in wireless sensor networks usually senses environmentally related data thus this may hint less importance of secure data transmission, in overall scheme, secure data communication is a part of the networks and secure communication should not be overlooked. If data are somehow tampered and data integrity can not be assured, upon data processing in sink node, incorrect conclusion propagating into improper decision may occur. This, in turn, may bring unintended or unexpected effects, not to mention disasters. However, if security is exerted aggressively, network lifetime may decrease quickly. Hence, formulating secure data communication in wireless sensor networks is difficult challenge and researches toward finding the best way of most-efficient security management are still progressing.

If the principle of minimum supervision is generalized over wireless sensor networks serving different purposes, it is necessary to review how this condition can be achieved by comparing the overall characteristics of sensor networks and limitations imposed. Because too aggressive security platform may not be well-suited for sensor networks and on the

*This paper was written during the study at Ajou University. Mikael Fernandus Simalango can now be reached at mike at amikelive.com

Scheme	Key Management	Pros	Cons
LEAP	pre-distribution, using individual,group,cluster, pairwise keys	Low communication overhead	Not proven for large sensor networks
PGCR	pre-distribution, future group keys	Minimum key establishment overhead, simple implementation	Not feasible in heterogeneous sensor networks, prone to security breach
SLIMCAST	level keys, data encryption	Low communication overhead, scalable	Significant overheads for sensor networks with dynamic topology
Wadaa	No explicit keys, anonymity analysis by data aggregation	Efficient communication with less overhead	Decision is error prone at node level

Table 1 Energy-aware key management schemes

other side, the security mechanism should be secure enough and resilient toward security attack, we bring the idea of adaptive security using historical data and predictive approach as an alternative to secure data transmission in wireless sensor networks with awareness of prolonging network lifetime.

The rest of this paper is arranged as follows: we reviewed some previous work concerning secure data transmission in wireless sensor networks. Then, we describe the main idea of adaptive security mechanism for secure sensor networks. We come up with some preliminary experiments and analysis. Finally, we summarize the work and propose some future research directives.

II. RELATED WORK

Discerning most researches about secure data dissemination in wireless sensor networks, two general approaches can be classified: preventive or pro-active, and passive approach. In preventive approach, secure data dissemination is cultivated by preventing data from being tampered. This can be achieved by using encryption and decryption process for data being transmitted or establishing key management for secure link creation between nodes. The passive approach, on the other hand, tries to react to known attacks while keeping network resilience high.

Preventive approach is realized through the implementation of key management and secure group communication. J. C. Lee *et al.* [7] reviewed various schemes and proposals for key management. Another article by P. Sakarindr *et al.* [8], which put emphasis on secure group communication, complemented the review.

Some of the work, however, only concerned about algorithm-centric implementation, thus in the following section, we will selectively present the compilation of key management and secure communication schemes with awareness of energy efficiency. The brief summary can be found in Table 1.

Zhu *et al*. [9] introduced LEAP (Localized Encryption and Authentication Protocol) for large-scale distributed sensor networks. The protocol is designed using hybrid approach where single key management scheme may not be suitable for various security requirements thus different packet types should be treated with different security services. There are four types of keys proposed in the scheme: individual, group, cluster, and pairwise shared keys. Individual key is a unique key used by a single node to communicate with the sink node. Group key is the key used for communication from sink node to all sensor nodes. Cluster key is

generated for communication among nodes located in the same cluster. Finally, pairwise shared key is used for establishing secure communications between neighboring nodes.

For establishing all types of the keys, a set of pre-distribution keys are used. Individual key is established using a function of seed and ID of the node. In pairwise shared key phase, nodes broadcasts their IDS to find their adjacent neighbors. Receiving node uses a function, which is seeded with initial key, to calculate the shared key for such neighboring area. Cluster key is distributed by the cluster head using secure pairwise communication and group key is distributed by a broadcast message from the sink-node through multi-hop, multi-cluster paths.

The advantage of this approach is low communication overhead hence the scheme is basically energy efficient. However, the article did not discuss the whole energy consumption at node level for implementing the four different keys.

Zhang and Cao[10] proposed PGCR (Pre-distributed and local Collaboration-based Group Rekeying) scheme which is aimed to prevent node capture and DoSS (Denial of Service on Sensing) attack. The gist of PGCR scheme is preloading group keys into sensor nodes prior to deployment. Future group keys can be determined from the preloaded keys thus decreasing the processing overheads. To key the future keys secure, the keys have to be protected by encryption with some polynomials, which are kept by some one-hop neighboring nodes. This, in turn, requires collaboration over all sensor nodes to retrieve the future keys and also to detect and protect the nodes against any attempt to compromise nodes. However, this approach has at least two drawbacks: the polynomials can be obtained by an attacker by searching only one-hop neighbor nodes of the victim and the attack itself can be initiated by compromising only a small number of one-hop neighbor nodes. Due to this limitation, some modifications were done to the scheme, for example CPCGR (Cascading PCGR), which distributes the polynomials to two or three neighboring nodes. RV-PCGR (Random Variance-based PCGR) was also proposed to strengthen the polynomials by adding random variance numbers to the polynomials.

The advantage of this approach is the ease of operation and reduced complexity for key management. However, due to the pre-distribution nature of future keys, rekeying is very limited. Moreover, because total collaboration of all nodes is required, this scheme may not be possible in real implementation, especially in case of heterogeneous sensor networks.

Huang *et al.* [11] initiated a new protocol named SLIMCAST (Secure Level key Infrastructure for MultiCAST), which is aimed to prevent DoS-based flooding attack through intrusion detection and deletion mechanism. This protocol ensures data confidentiality via hop-by-hop encryption. SLIMCAST protocol divides a group routing tree into levels and branches at cluster level. A level key protects communication among nodes in each level in each branch of the group tree. This protocol also enables secure data aggregation from downstream nodes to upstream nodes by encrypting the data with level keys that are shared between child and parent nodes. If duplicate packet is detected, for example, packet originated from the sibling node, it will be discarded to reduce redundant bandwidth and power consumption.

The advantage of this approach is the low communication overheads and power consumption. Performance also doesn't degrade substantially if the group size increases. However, when membership

changes rapidly and repeatedly, performance is degraded significantly.

Wadaa et al. [12] proposed an energy-efficient protocol to address anonymity in wireless sensor networks. In this protocol, a network is divided into clusters. In each cluster, two kinds of activities are defined: intracluster activity and intercluster activity. For intracluster activity, a transaction instance manager acts as the destination of sensor readings from various nodes. The manager will then collects all node reports and formulates TIR (Transaction Instance Report). For intercluster activity, TIR is sent by the manager to the sink node through hop-by-hop manner. The protocol will formulate the anonymity problem and eliminate the minimum number of nodes that cause the maximum loss of sensor readings.

The advantage of this approach is energy-efficient scheme. Network performance also does not degrade if the group size increases. However, the scheme did not analyze or prove anonymity level per transmission.

III. ADAPTIVE SECURITY MECHANISM

The idea of adaptive security mechanism originates from a controversial idea that security level is predictable. In a network where incident or attack rarely occurs, at least two opinions can be inferred. The first one is data transmitted in the network is not sensitive thus information may not be beneficial to interested parties. The latter is security in the network is maintained so that it's safe from incoming attack.

The idea can be expanded as follows. Given a wireless sensor network S with N number of nodes. The network can be arranged by clusters thus communication to sink node is handled by cluster head or the network is primitive where nodes communicate using hop-by-hop manner to the sink node. We assume a periodic aggregation function is operated over the network. The aggregation method can be either through simple aggregation like in [6] or conducted by mobile agent like in [13]. In the aggregation process, not only sensor readings are collected but also energy level. The layout of a sensor node in the network can resemble Figure 1. It is shown in the figure that power unit reports its level to processing unit and CPU may coordinate with communication subsystem to forward the information along with sensor readings.

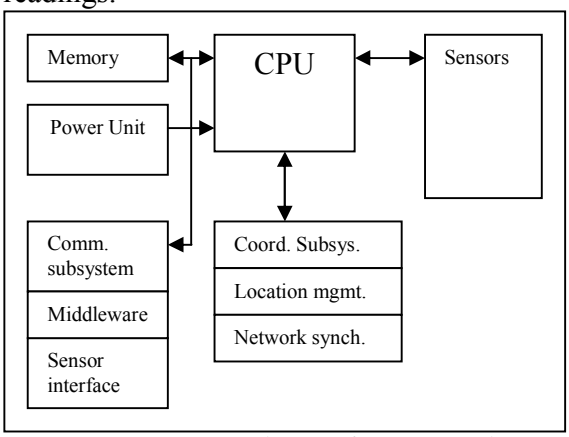

Figure 1 System layout of a sensor node

In case identifiable attack occurs in the network, sink node should also be aware through notification from attacked node or nodes adjacent to compromised node. Sink node should also maintain the history of security threats and attacks. If history of the network did not reflect any critical attack, security level can be adjusted to conserve energy in regard to current security level respectively.

We will now define t_s as period of sampling and T as total time of sampling. We will compute security level as the probability for an attack to occur. Markov chain and fuzzy model are very interesting models in computing the probability. However, we will reduce the complexity by applying weighted probability value.

We define ρ as the probability of an attack to occur. High ρ refers to history of past attacks and low ρ hints scarcity of attacks. We also define ρ_{th} as the threshold value for less secure communication where we expect to conserve energy if communication between nodes is executed at this state. We then assume δ as data sensitivity where $\delta = 0$ denotes insensitive data and $\delta = 1$ denotes very sensitive data. Average energy level is denoted as Ω_{av}. Subsequently, the value of current ρ is computed as the following:

$$\rho = \sum_{i=1}^{N} i\alpha^{N-i}(1-\alpha)^{N-i+1}\frac{t_s}{T}(1-F) \ldots (\text{eq. 1})$$

From above equation, α is the weighing factor that satisfies $0 < \alpha < 0.5$. The variable F denotes logical state of i-th sampling. F = 1 means that attack occurs during the sampled time and F = 0 refers to no attack.

Now we will use the following algorithm to decide if security level can be adjusted:

Algorithm 1

```
If energy_level decreases and
energy_level is less than threshold_level
Then
     If  attack_probability is low
     Then
        use least_secure_comm
     Else if attack_probability is
     high and sensitivity is low
     Then
         use less_secure_comm
     Else
         raise alert
EndIf
```

The above algorithm uses attack probability obtained from eq. 1 as a parameter for security adjustment strategy. If sink node detects that average energy level in the network goes below the threshold value, it should perform security adjustment by computing the attack probability and reinforcing security policy. For low attack probability and higher attack probability for less sensitive data, less secure communication can now be established over the network. However, when the attack prevalence is high and data is sensitive, an alert should be raised so that manual inspection can be conducted over the network.

For the implementation, we are interested in LEAP and SLIMCAST approaches. We combine both and then modify the scheme to fit the adaptive strategy. We achieve security through two methods: encryption and key management.

For key establishment, two types of keys are used: network keys and level keys. Level keys have the same functionality with those in SLIMCAST. Level keys that are shared between child and parent nodes are used to encrypt data while it is being forwarded to the sink nodes. To establish communication between nodes, prior to deployment, a global network-wide keys are distributed and nodes select k number of keys from the total of M generated keys and a key x which is the same for all the nodes in the network. Subsequently, hop-by-hop communication is established if two nodes share the same key of their global key repositories.

A most secure link is associated with secure connection and data encryption. Less secure link is associated with secure connection without data encryption. At last, least secure link refers to link establishment between nodes participated in initial network key distribution.

The communication protocol should now enable SEC_LEVEL in its header. This header is used to notify nodes about security pattern for future communication. Sink node should broadcast message to all nodes in the network to notify that security has been adjusted and node should comply to the new policy accordingly. As the broadcast path varies and time for the message to arrive at

outer nodes is longer than inner nodes, an SEC_ACK mechanism should also be implemented in the protocol.

After receiving the message, node should send SEC_ACK to sink node in order to confirm that such node is aware of the policy change and ready to implement the new policy. A node should put its ID in the acknowledgement response to prevent duplicate ACKs and to enable sink node to calculate the rate of policy change awareness across the network. Figure 2 shows how the protocol can be implemented in a sensor network.

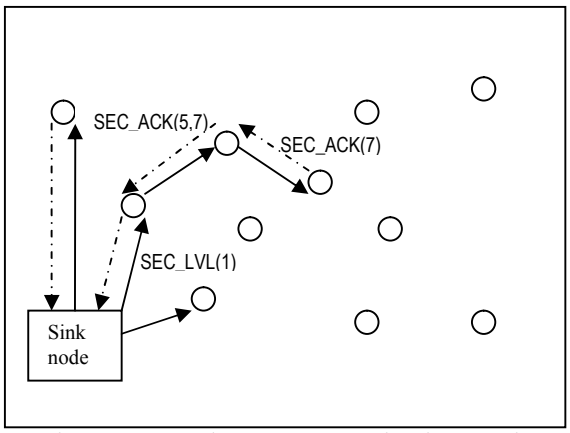

Figure 2 Example SEC_LEVEL implementation

IV. SIMULATION AND DISCUSSION

Based on investigation in [14], [15], and [16], we decided to use Castalia[18] for the simulation. Castalia is a simulator tailored for wireless sensor network based on OMNET++[17]. Currently it is running on command line mode hence data acquisition and analysis still have to be carried out manually.

First simulation is executed to measure the effect of secure communication to energy depletion rate. We then assume a network consisting of N nodes. Key establishment and management add ε overhead for each node. For the data transmission, each node periodically sends q bytes of data (= 50 bytes) to the sink node. Data are forwarded to the sink node through hop-by-hop manner.

Figure 3 shows the result of the experiment. From the diagram, it can be seen that for bigger number of nodes, energy depletes slightly quicker. This can be caused by more complex key management resulting in more overhead for establishing the link and forwarding data. However, the result is intuitive and aligned to our expectation. We can see that overhead cuts network lifetime significantly. This is the drawback of security we want to deploy over the network. By applying the adaptive approach, we expect to reduce the total overhead thus the slope for energy depletion in the time diagram will be less in magnitude.

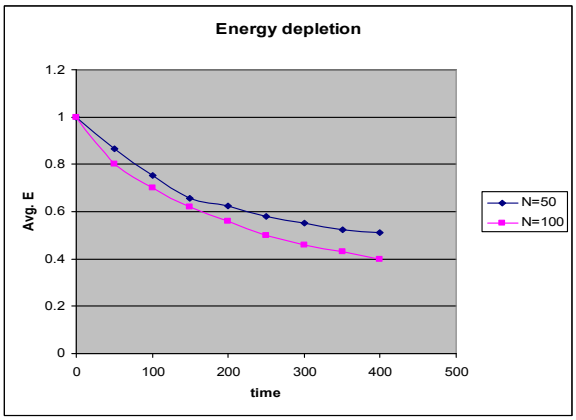

Figure 3 Energy depletion for processing overhead

The first experiment is very basic since we only analyze the effect of overhead from security implementation to the energy level. Subsequent simulation should model data processing at the sink node and the whole adaptive security mechanism. However, since the simulator currently does not implement such security level protocol which means it has to be developed as a new module, we have not been able to provide simulation results for the protocol implementation in wireless sensor network. This, in turn, invites similar researches from interesting parties to

prove this concept and bring it into real implementation.

V. FUTURE WORK

Since we still need more validation to our concept, we accentuate the necessity of various experiments with different schemes. The experiments should be aimed to achieve most efficient energy usage by taking into account security of overall networks. We are also interested in simulating the networks using motes and TinyOS to obtain the empirical result of this concept.

VI. CONCLUSION

In data communication, security is an important aspect to be considered including in wireless sensor networks. However, energy-constraint in such networks leads to intricate security policy and management. We offer adaptive security level mechanism concept that will enable the network to conserve the energy when energy level goes below certain threshold value. Further experiments are invited to prove this concept and assess the feasibility of the implementation in large wireless sensor networks.

REFERENCES

[1] R.N. Murty, G. Mainland, I. Rose, A. R. Chowdhury, A. Gosain, J. Bers, M. Welsh. CitySense: An Urban-Scale Wireless Sensor Network and Tesbed. In *Proceeding of IEEE International Conference on Technologies for Homeland Security*. 2008

[2] G. W.-Allen, K. Lorincz, J. Johnson, J. Lees, M. Welsh. Fidelity and Yield in a Volcano Monitoring Sensor Network. 2006

[3] K. Srinivasan, P. Dutta, A. Tavakoli, P. Levis. Some Implications of Low Power Wireless to IP Networking. In *The Fifth Workshop on Hot Topics in Networks (HotNets-V)*. 2006

[4] M. Shi, X. Shen, Y. Jiang, C. Lin. Self-Healing Group-Wise Key Distribution Schemes with Time-Limited Node Revocation for Wireless Sensor Networks. *IEEE Wireless Communications Magazine*. October 2007

[5] P. Traynor, G. Cao, T. L. Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceeding of Wireless Communications and Networking Conference (WCNC)*. 2006

[6] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi. In-Network Aggregation Techniques for Wireless Sensor Networks: A Survey. *IEEE Wireless Communications Magazine*. April 2007

[7] J. C. Lee, V. C. M. Leung, K. H. Wong, J. Cao, H. B. Chan. Key Management Issues in Wireless Sensor Networks: Current Proposals and Future Developments. IEEE Wireless Communications Magazine. October 2007

[8] P. Sakarindr, N. Ansari. Security Services in Group Communications over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks. *IEEE Wireless Communications Magazine*. October 2007

[9] S. Zhu, S. Setia, S. Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In *Proceeding of 10th ACM Conference on Computer and Communication Security*. October 2003

[10] W. Zhang, G. Cao. Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach. In *Proceeding of IEEE INFOCOM'05*. March 2005

[11] J.-H. Huang, J. Buckingham, R. Han. A Level Key Infrastructure for Secure and Efficient Group Communication in Wireless Sensor Networks. In *Proceeding of 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*. September 2005

[12] A. Wada *et al*. On Providing Anonymity in Wireless Sensor Networks. In *Proceeding of 10th International Conference on Parallel and Distributed System*. July 2004

[13] M. Chen, S. Gonzalez, and V. C. M. Leung. Applications and Design Issues for Mobile Agents in Wireless Sensor Networks. In *IEEE Wireless Communications Magazine*. December 2007

[14] Y. Xue et al. Performance Evaluation of NS-2 Simulator for Wireless Sensor Networks. In *Canadian Conference on Electrical and Computer Engineering*. 2007

[15] C. Mallanda et al. Simulating Wireless Sensor Networks with OMNET++. 2005

[16] T. M. Tam. A Survey on Wireless Sensor Network Simulators. 2007

[17] OMNET++ Discrete Event Simulation System. http://www.omnetpp.org

[18] Castalia Simulator for Wireless Sensor Network. http://castalia.npc.nicta.com.au