This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2009 proceedings

Dynamic Resiliency Analysis of Key Predistribution in Wireless Sensor Networks

Ahmet Onur Durahim
Computer Science and Engineering
Sabanci University, Istanbul, Turkey
durahim@su.sabanciuniv.edu

Albert Levi
Computer Science and Engineering
Sabanci University, Istanbul, Turkey
levi@sabanciuniv.edu

Abstract— **Wireless sensor networks have been analyzed for more than a decade from operational and security points of view. Several key predistribution schemes have been proposed in the literature. Although valuable and state-of-the-art proposals have been made, their corresponding security analyses have not been performed by considering the dynamic nature of networking behavior and the time dimension. The sole metric used for resiliency analysis of key predistribution schemes is "*fraction of links compromised*" which is roughly defined as the ratio of secure communication links that the adversary can compromise over all secure links. However, this metric does not consider the dynamic nature of the network; it just analyzes a snapshot of the network without considering the time dimension. For example, possible dead nodes may cause change of routes and some captured links become useless for the attacker as time goes by. Moreover, an attacker cannot perform sensor node capturing at once, but performs over time. That is why a methodology for dynamic security analysis is needed in order to analyze the change of resiliency in time a more realistic way. In this paper, we propose such a dynamic approach to measure the resiliency of key predistribution schemes in sensor networks. We take the time dimension into account with a new performance metric, "*captured message fraction*". This metric is defined as the percentage of the messages generated within the network to be forwarded to the base station (sink) that are captured and read by the attacker. Our results show that for the cases where the static fraction of links compromised metric indicates approximately 40% of the links are compromised, our proposed captured message fraction metric shows 80% of the messages are captured by the attacker. This clearly proves the limitations of the static resiliency analysis in the literature.**

Keywords: message capture; node capture; resiliency analysis; sensor networks; minimum cost routing; key predistribution

I. INTRODUCTION

Wireless sensor networks (WSN) consist of large number of small devices, called sensor nodes, which sense and process information related to a particular application [4]. Sensor nodes are battery powered devices with limited computation and short range communication capabilities. The ultimate aim in a sensor network is to transfer the sensed information to a base station (sink) via multi-hop network. In-network data processing, e.g.. data aggregation, is also a common practice.

Depending on the application, confidentiality and/or authenticity of the data may be an important design criteria. In-network data processing requirements cause link-by-link data processing and consequently setting up pairwise cryptographic keys among the neighboring sensor nodes. In the literature, there are several key distribution schemes proposed for sensor networks [1, 8, 9, 10, 11] as will be described in Section II. The resiliency of these schemes is analyzed by the amount of secure links compromised as the attacker capture nodes in the network. An implicit assumption in this type of resiliency analysis is that the resiliency effect of each link is the same. However, this is not correct. Some links may not be used at all due the underlying routing mechanism; some links, especially the ones close to the sink, are more critical than the others since more messages pass through those links. Moreover, sensor networks are dynamic ones such that some nodes malfunction or deplete their batteries or some links may be dropped due to hidden node problem. In such cases, new routes are established. That means, the links which carry data my change during the lifetime of the network.

In this paper, we envision that the existing resiliency analyses of the key distribution schemes in the literature are quite limited. They do not reflect the actual damage of node capture since the network analysis is done in a static way without considering the effects of the real networking behaviors. Dead nodes and route changes should also be considered in a dynamic way in the time dimension. Moreover, the existing analyses assume that the attacker captures all nodes at the same time, which is totally unrealistic. In point of fact, node capture is performed over the time. Last, but not the least, the real damage of node capture must be measured as a function of *messages* captured by the attacker, not as the links compromised. In this paper, we address the abovementioned dynamicity problems of resiliency analysis of key predistribution schemes in WSNs. We consider the dynamic networking behavior in simulations and propose a novel metric, *captured message fraction*, as a realistic measure of attacker's harm on the network. In that respect, we measure the fraction of messages captured by the attacker. We compare the results of our dynamic analysis with classical static one. Our results show tremendous deficiency of static analyses in perception of the harm caused by attackers.

The rest of the paper is organized as follows. Section II gives background information and sketch of our contribution. Section III explains the details of our dynamic simulation model. In Section IV, the performance evaluation is given. Section V summarizes the conclusions reached by this work.

This work is supported by Scientific and Technological Research Council of Turkey (TUBİTAK) under grant 104E071

978-1-4244-3435-0/09/$25.00 ©2009 IEEE

II. Background Information and Sketch of Contribution

A. Key Distribution in WSNs

In order to fulfill the confidentiality and authentication requirements of the data transferred in a sensor network, pairwise keys must be established. The deployment of sensor nodes over the field is considered as random, which makes it impossible to know which nodes will be neighbors of each other prior to the deployment. Thus, equipping the large amount of sensor nodes with all possible pairwise keys requires a huge amount of key memory. This is not a feasible approach. Using public key cryptosystems [5, 6] for key establishment is costly for computationally limited sensor nodes. In the WSN literature, the common approach for key distribution is the *random key predistribution* schemes in which reasonable amount of keys or keying materials are distributed to each sensor node prior to the deployment. This idea is first proposed by Eschenauer and Gligor [1]. There are three phases in Eschenauer and Gligor (EG) random key predistribution scheme. In *key pre-distribution phase*, each sensor node is given a set of keys from a large pool of keys randomly. In *shared key discovery phase*, each neighboring sensor node pair try to find a common key between their sets of keys. If one is found, then it is used as their link key. If not, this node pair executes the *path key establishment phase* in which the pairwise key is established with the help of other secure neighbors over a few hops at the cost of more communications. In the literature After EG scheme, some other key distribution schemes and improvements are proposed in the literature. A scheme taking deployment knowledge into account is proposed by Du et al. [8]. Improvements over [1] are proposed by Chan et al. [9]. Du et al. [10] and Liu and Ning [11] proposed other random key predistribution schemes.

B. Routing in WSNs

In the literature, there are several well-known routing protocols which try to reduce the energy consumption due to message flow from individual sensor node to the sink. They are classified into four basic categories as discussed in [3]: Data centric protocols such as Flooding and Gossiping [12], Directed diffusion [13]; Hierarchical protocols such as LEACH [14]; Location based protocols such as GAF [15], GEAR [16]; and Network Flow and QoS aware protocols such as Minimum Cost Forwarding [2].

In those protocols, security is not considered by design. On the other hand, secure routing [17] protocols are proposed which consider security at the design level. These include SecLEACH [18] and TTSR [19].

C. Limitations of Resiliency Analysis in the Literature

Sensor nodes are susceptible to certain types of attacks, such as impersonation, message interception, and fabrication, when they are deployed into hostile areas of operation. The nodes may be captured by an attacker whose aim differs according to the attacker scenario. Attacker obtains the keys that are stored in the captured node's key ring and use them in order to eavesdrop on messages as well as transmitting false information to other nodes. This, of course, is possible if the captured sensor node does not have tamper proof hardware. In fact, in most sensor networks, simple nodes are used and expensive tamper resistance hardware solutions are not implemented.

Resiliency analysis of both key distribution and routing schemes has been centered around the survivability of the network in presence of adversary capturing nodes. In those analyses, *fraction of links compromised* has been used as the main metric for key predistribution schemes. In the literature, this metric is defined as the fraction of additional secure communication links among uncaptured nodes that an adversary can compromise based on the information retrieved from previously captured nodes [8]. In other words, this metric considers the links among the uncaptured nodes. Since the same keys may be reused in different areas of the network, capturing of a node and its keys cause some other links in different parts of the network to be compromised as well.

The resiliency analysis of the key predistribution schemes proposed in the literature using this fraction of links compromised metric is actually a *static* one such that it does not consider the dynamic nature and operational characteristics of WSNs as detailed below:

- The classical fraction of links compromised metric implicitly, and wrongfully, assumes that all secure links are of the same importance level. Therefore, the amount of harm caused by the compromised links cannot be measured precisely. Due to the operational characteristics of the network and the routing schemes employed, there might be cases where some links are not used and some links are used extensively since they are close to the sink.
- The sensor nodes may deplete their energies as they transmit and receive data packets. In such cases, the routing changes dynamically over the time. In the classical resiliency analysis of proposed key distribution schemes, this fact is not taken into account since the sensor network is not simulated over time considering such operational characteristics.
- Energy depletion also affects the eavesdropping on the transmissions. This is due to the fact that a node, of which encryption keys are at the hand of the adversary, may die and further transmission would be carried over other nodes.

D. Our Contribution and Assumptions

As detailed in the previous subsection, fraction of links compromised is not a suitable security metric for resiliency analysis due to the dynamic nature of WSNs. In order to measure the real harm of node captures, one needs to perform network simulations by considering the operational characteristics of the network and dynamic changes in routing over time. In other words, the time dimension should also be incorporated in the analyses which is lacking in classical analyses in the literature. In this paper, we address these abovementioned issues via *network simulations*. We define the dynamic equivalent of the fraction of links compromised metric. We also propose and analyze a novel and more realistic metric which takes dynamic nature of the network

structure as well as the key management into consideration. This metric, called *captured message fraction*, is basically defined as the fraction of messages obtained by the attacker over all messages transferred in the network. We analyze the changes of these metrics with respect to time for different key ring sizes, message generation and node capture rates. Our simulation results show that there is an important gap between the classical metric and the proposed captured message fraction metric.

We consider the EG scheme [1] as the underlying sample random key predistribution model in our analysis. We do not propose an improvement of EG scheme, since our aim in this paper is to show the limitation of classical resiliency analyses rather than improving the key predistribution schemes.

In our simulation model, security threat comes from the fact that a node can be physically captured by the attacker. Moreover, we do not assume tamper-proof hardware to protect the private information in a tiny and simple sensor node since this would be an expensive security measure. Therefore, the keys of a captured node are assumed to be compromised by the attacker. On the other hand, the sink is assumed to be in a safe place and cannot be captured.

III. SIMULATION MODEL

In this section, we describe our simulation model including the key distribution, routing and other network operations.

A. Random Key Predistribution and Key Establishment

We use Eschenauer and Gligor's [1] EG random key predistribution scheme in our simulations. This scheme consists of three phases: (i) key pre-distribution, (ii) shared key discovery and (iii) path key establishment. Path key establishment phase is not put into operation in our simulation model since the resiliency analysis considers only the direct keys established in the second phase.

Key predistribution phase: An offline key distribution center randomly picks k keys for each node out of a large *key pool* that consists of P distinct keys. Each key has an identifier. Selected keys along with their key identifiers are loaded into the memory of the sensor node before the deployment. These stored keys constitute the node's *key ring*.

Shared-key discovery phase: After the nodes are deployed onto the sensor network area, each node discovers its neighbors, which are the nodes within the communication range. Then, each sensor node broadcasts the list of its key identifiers (not the keys themselves) of its key ring in cleartext. After that, each neighboring node pair finds out whether they share a common key in their key rings by comparing local key identifiers and the ones received from its neighbor. If one such key is found, then it is used as the link key between these two neighboring nodes. Attacker cannot mount an attack in this phase, since it does not know the values of the actual keys corresponding to the key identifiers.

The parameters of key pool size, P, and key ring size, k, are important since it determines the probability of two neighboring nodes sharing a key. In [1], this probability is called as *local connectivity*. It is desirable to have high local connectivity with increased k/P ratio, but increased local connectivity makes the system less resilient since more keys are reused in different parts of the network. Thus, there is a tradeoff here. Moreover, having a large k value may not be feasible due to the memory limitations of sensor nodes.

In our simulations we consider different k/P values in order to obtain the desired local connectivity for which resiliency and message capture is to be explored.

B. Routing

In our sensor network model, minimum cost forwarding protocol [2] is selected as the routing protocol to be implemented. In this protocol, the cost criteria can be taken as hop count, energy consumption, and/or delay, etc. Minimum cost forwarding is based on the *cost field* phenomenon. Cost field of a node is defined as the minimum cost from that node to the sink on the optimal path.

In route establishment phase, similar to minimum cost forwarding protocol explained in [2], our network nodes construct minimum cost field based on their distance to the base station node. In our model, it is assumed that all nodes know their relative positions to their neighbors. In addition, at the center of the sensor network area, there is a sink node which is more powerful than other sensor nodes, may be a laptop-class sensor node. This sink plays the role of a base station to where all of the packets generated within the network are to be forwarded.

In order to establish routing, firstly, all nodes that are within the transmission range of the sink set their parent node as the sink node and send their messages directly to it. Then, those nodes that have sink node as their parents broadcast this information to their neighboring nodes. Afterwards, each one of the remaining nodes sequentially finds a parent by considering the distances of the neighboring nodes that are within the transmission range. Recursively, minimum cost field is constructed for each node.

C. Sensor Network Operations

1) Re-routing to circumwent dead nodes: During the operation of the network, some nodes deplete their energy and die. In such a case, all predecessors of the dead node try to find a new parents in order to forward their outgoing messages. To do so, a child node checks its neighboring nodes of which it shares at least one key. If there are one or more such nodes, it chooses one with the least routing cost by applying the same logic as the one used in the initial routing protocol. If there is no such a node, the child node is marked as disconnected and its children try to find a new path. This logic continues recursively until all the child nodes find their corresponding parents. If no parent could be found by a child node, then this node becomes disconnected from the network and does not generate and/or forward messages any more.

2) Message Generation and Forwarding: In our simulation model, message forwarding is performed over the routes established previously. Moreover in our simulation model, the time dimension is divided into epochs of 100 milliseconds. In

each time epoch, each sensor node first determines whether or not to generate a new message to be sent to the base station. If generated, this new message is put into the node's outgoing buffer along with the messages received from the children nodes. Finally all the messages in the outgoing buffers are forwarded towards the next hop.

In our simulation model, sensor nodes decide whether or not to generate a new message probabilistically. This probability is determined using the system parameter *message generation rate*, R_g, which is defined as the average number of messages generated in a time unit. We use messages/minute as the unit of R_g. Given that one time epoch is 0.1 seconds, the probability of a node to generate a new message during an epoch is calculated as R_g /600 in our simulations.

Message forwarding is performed irrespective of capture status of the next node (whether it is captured or not). Thus, if the next node is a captured one, then all the outgoing messages are captured and read by the attacker.

3) Node and Message Capture: In our attack model, there is an active attacker that captures nodes and illegally decrypts messages that were encrypted with the compromised keys obtained from the captured nodes. We employ a random capture model in which the attacker picks the nodes to be captured at random locations without any bias. Moreover, we assume that the attacker or its agent is capable of listening to the entire network and in order to obtain the messages that are sent and received by uncaptured nodes.

The attacker in this model captures a node in each time epoch probabilistically. This probability is derived from another system parameter called the *node capture rate*, R_c. This parameter is defined as the average number of nodes captured by the attacker per hour. Given that one time epoch is 0.1 seconds, the probability of the attacker to capture a node in an epoch is calculated as R_c /36000 in our simulations.

It is assumed that base station would never be captured by the attacker which would result in total network collapse.

Whenever attacker captures a sensor node in a time epoch, it learns and saves the keys in captured node's key ring. In addition, attacker starts capturing and reading encrypted messages that pass through this currently captured sensor node. Moreover, if the keys learned in this way are used to secure other links between uncaptured nodes in the other parts of the network, the encrypted messages sent over these links are also compromised by the attacker.

In our network model, the attacker may capture the same message more than once if more than one links are compromised en route. Duplicate message capture can occur since in our model there is no real-time attack detection and prevention logic. It is assumed that the attacker modifies none of the captured nodes and messages; thus, network operates as if there is no attack. However in our model, the attacker, in cooperation with all captured nodes, records message ids of captured messages in order not to unnecessarily decrypt and store it again and again. In this way, we avoid double counting of the captured messages and accurately generate our results on message capture statistics.

IV. Performance Evaluation

We perform several network simulations in order to understand the resiliency behavior of WSNs against node captures while the network is dynamically operating over time. We consider three important parameters in our simulations: *node capture rate*, *message generation rate*, and *key ring size*. All simulations are reported with respect to time (i.e. the *x* axis is the simulation time).

In all simulations, the sensor field is taken as 1000m × 1000m area. The number of nodes deployed over this area is 10,000. Communication range of a node is taken as 40m. The keys are drawn from a key pool in which there are 100,000 distinct keys. Energy capacity of the nodes is determined such that each sensor node is able to forward a total of 250,000 messages. One simulation time unit (epoch) is taken as 100 milliseconds. Simulation code is developed in C++ using MS Visual Studio 2005 on Windows XP running on an Intel Celeron 1.7 GHz M processor.

A. Performance Metrics for Resiliency

We explore the effects of different values the abovementioned three parameters on *fraction of links compromised* and *captured message fraction* metrics.

The metric of *fraction of links compromised* was defined in Section II.C by referring its classical definition in the literature. We use this classical definition in our simulation model, but as a different feature, instead of the number of nodes captured, we show its change over time dynamically.

The metric of *captured message fraction* is the unique feature of our model. It is defined as the number of encrypted messages read by the attacker as a result of node and consequently link key captures over all encrypted messages sent over the network. This metric gives a better understanding of the harm caused by the attacker since the ultimate aim of link captures is nothing but reading the encrypted messages. As mentioned in Section III.C.3, each message generated in the network is counted only once. In this way, the results obtained become more realistic.

B. Effect of Key Ring Size

We perform simulations for key ring size values of 300, 400, and 500 keys that correspond to 0.60, 0.80 and 0.92 local connectivity, respectively. In these simulations, message generation rate and node capture rate are fixed to 1.5 messages per minute and 8 nodes per hour, respectively. The results of both metrics (message capture fraction and fractions of links compromised) are depicted in Figure 1. As can be seen from this figure, in both metrics, capture fractions increase with the increasing values of key ring size (and consequently local connectivity).

Besides, it is also deduced from Figure 1 that for each key ring size, fraction of links compromised metric increases linearly with respect to simulation time. However, percentage of captured messages metric shows logarithmic increase (i.e. rate of increase reduces). Moreover, it is also observed that there is significant gap between the captured message fraction and fraction of links compromised for each key ring size. The

implications of these last two observations will be discussed in more detail in the next subsection.

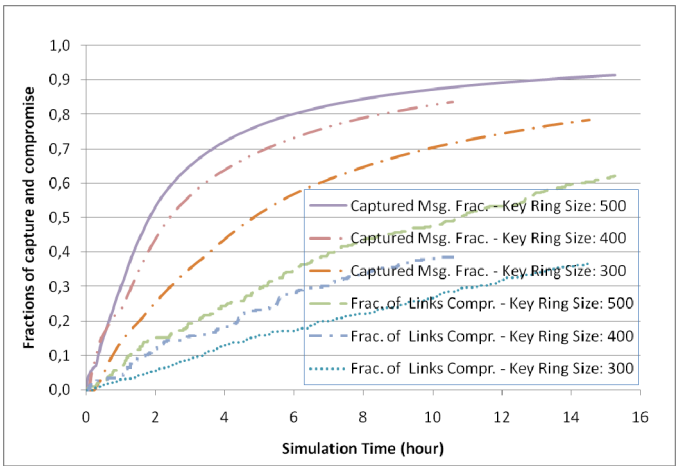

Figure 1. Resiliency metrics w.r.t. Simulation time for different key ring size values

C. Effects of Message Generation and Node Capture Rates

We also analyzed the effects of message generation rate and node capture rate on the resiliency metrics. In those analyses, the key ring size is fixed to 300.

Figure 2 shows the change of the fraction of links compromised with respect to simulation time for three different node capture rates: 8, 12 and 24 nodes per hour. In those simulations message generation rate is taken as 1.5 messages per minute for each node within the network. As can be seen in Figure 2, the linear increase behavior of fraction of link compromised with respect to time does not change as the node capture rate changes. When node capture rate is increased, it leads to an increase in fraction of links compromised as expected. Moreover, an increase in node capture rate results in nearly equal rate of increase in the fraction of links compromised (e.g. doubling node capture rate leads to an approximately 100% increase in the fraction).

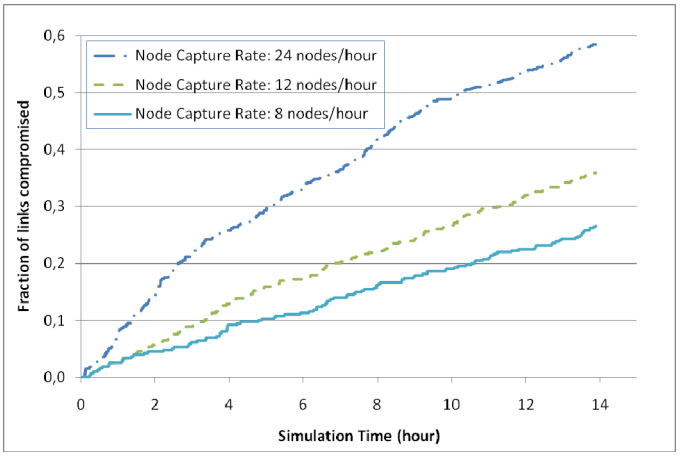

Figure 2. Fraction of links compromised wrt. simulation time for different node capture rates

Figure 3 shows the change in the fraction of captured messages with respect to simulation time for different node capture rates. The same parameters as Figure 2 are used here as well. Different than the other metric, fraction of captured messages metric exhibits a logarithmic increase behavior especially for high node capture rates. For low capture rates, the increase is still logarithmic, but the rate of increase does not change so rapidly. This logarithmic increase behavior indicates that the effect of node captures and consequently link compromises is more severe at the beginning of the attack. As the attacker continues to capture more nodes, his/her marginal gain reduces. This result is one of the important conclusions of our proposed analysis model since it cannot be seen by analyzing the fraction of links compromised metric only.

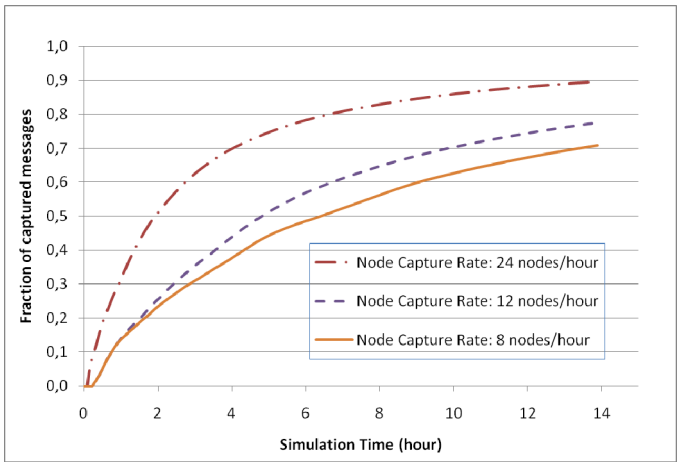

Figure 3. Fraction of captured messages w.r.t. simulation time for different node capture rates

We also examine the effect of message generation rate on both metrics. In these simulations, node capture rate has been fixed to 12 nodes per hour. Simulations are performed for four different message generation rates ranging from 0.75 to 6 messages per minute. Corresponding results are given in Figure 4. As it is seen from this figure, message generation rate does not have significant effect both on the fraction of links compromised and on the fraction of captured messages. This behaviour is expected for fraction of links compromised since the message generation is independent of node and link captures. However, it is quite unintuitive not to have a change for the fraction of message capture. Here, of course, the amount of messages captured increases with increasing message generation rate, but the total number messages also increases in the same rate so that the fraction remains the same.

Although it can be observed in other figures, the gap between two metrics is best visualized in Figure 4. The fraction of captured messages is always higher than the fraction of links compromised. The proportional difference is higher at the beginning; 10% link compromise results in 40% of the messages captured by the attacker (at ~200 minutes). The proportional difference reduces in time, but the difference is still significant. For example, when the 40% of the links are compromised, 80% of the messages become captured by the attacker (at ~900 minutes). This significant gap implies that the resiliency intuition of the fraction of links compromised metric is misleading. The actual harm of the attack on the

network, in terms of messages captured, is much higher than what the fraction of link compromise value implies. This is another important result obtained from our dynamic analysis model.

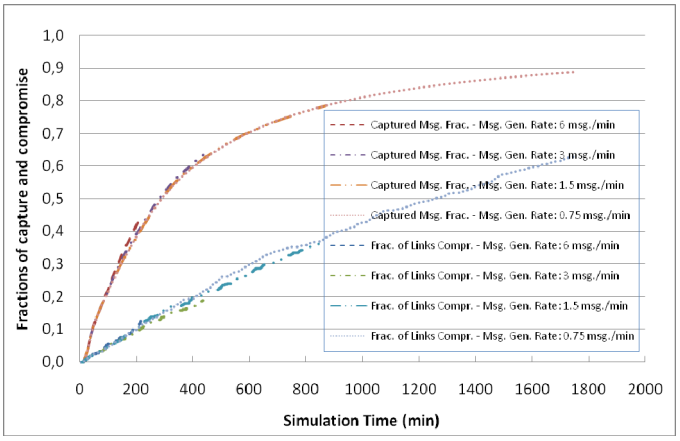

Figure 4. Resiliency metrics w.r.t. simulation time for different message generation rates

One may easily see from Figure 4 that simulations with low message generation rates run longer than others. This is due to the fact that: (i) we plot the results until the sink becomes disconnected from the rest of the network; (ii) for smaller message generation rates, the batteries of the nodes last longer since less messages are forwarded in the network resulting longer lifetime.

V. Conclusions and Future Work

In this paper, we propose a simulation model for dynamic resiliency analysis of wireless sensor networks against node captures and show the deficiencies of the existing analysis models. We propose a novel and realistic resiliency metric called *message capture fraction* and analyzed it dynamically in the time dimension. We compare the results with the classical resiliency metric of *fraction of links compromised* and see that the classical metric does not realistically show the harm of the node capture attacks. We obtained two important results that cannot be obtained using classical analysis techniques: 1) the real effect of the attack is more severe at the beginning and the rate of increase of the harm reduces in time; 2) the fraction of links compromised metric is misleading such that it is much smaller than the fraction of captured messages.

Fraction of links compromised metric used in classical resiliency analysis techniques is an unrealistic one since it does not take into account actual routes. In fact, compromising a node's keys is harmful only when it is used to encrypt messages during message forwarding. However, this fact is not considered in the classical techniques using fraction of links compromised metric.

We use EG random key predistribution scheme [1] and minimum cost forwarding protocol [2] in our analyses. As future work, we plan to adapt our model to different key distribution schemes and routing protocols.

References

[1] L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. Ninth ACM Conf. Computer and Comm. Security, Oct. 2002.

[2] F. Ye, et al., "A Scalable Solution to Minimum Cost Forwarding in Large Scale Sensor Networks," in the Proceedings of International Conference on Computer Communications and Networks (ICCCN), Dallas, TX, October 2001

[3] K. Akkaya, M. Younis, “A Survey of Routing Protocols in Wireless Sensor Networks,” in the Elsevier As Hoc Network Journal, Vol 3/3 pp. 325-349, 2005.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, August 2002.

[5] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, pp. 644–654, November 1976.

[6] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, “Spins: Security protocols for sensor networks,” in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 189–199.

[8] W. Du, J. Deng, Y.S. Han, S. Chen, P.K. Varshney,“A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,” IEEE INFOCOM 2004.

[9] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.

[10] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pairwise key predistribution scheme for wireless sensor networks,” in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42–51.

[11] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 52–61.

[12] S. Hedetniemi and A. Liestman, “A survey of gossiping and broadcasting in communication networks,” Networks, Vol. 18, No. 4, pp. 319-349, 1988.

[13] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000.

[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in the Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[15] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in the Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’01), Rome, Italy, July 2001.

[16] Y. Yu, D. Estrin, and R. Govindan, “Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks,” UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.

[17] 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, Sept. 2003.

[18] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro. “SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks”. Fifth IEEE International Symposium on Network Computing and Applications (NCA’06)

[19] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, “Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks,” IEEE Transactions on Wireless Communications Vol. 6, Issue 9, pp. 3395–3401, Sept. 2007.