Modeling Attacks In Wireless Sensor Networks

Chinya V. Ravishankar
University of California, Riverside.

1 Introduction

Compromises in sensor networks are a serious problem, but no general framework exists for modeling compromises. Sensors may be static or mobile, and are often deployed in groups for reliability [1, 2, 3]. One must ensure the integrity of both data reports and that of data in transit [4, 5, 6, 7]. When two sensors do not share a preloaded key, they may establish a *path key* using an intermediary. The resilience of a key establishment scheme is inversely related to the number of path keys it creates.

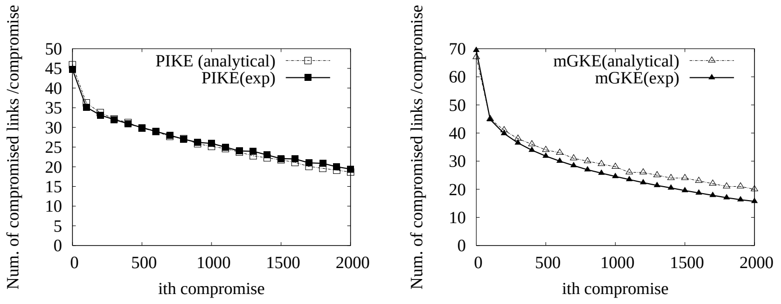
Previous schemes [8, 9, 10, 11, 1, 2, 12] have analyzed *random* attack, in which attackers randomly compromise sensors. A *selective* attack [2, 3], however, chooses targets to maximize the benefits of attack. An adversary targeting a certain region will target sensors in it. Similarly, an adversary may target sensors that hold the largest numbers of uncompromised keys, to maximize the number of key compromises at the next attack step. As shown in [3], selective attacks are deadlier than random attacks. To compromise 50% of the communication links among uncompromised sensors in a 10,000-node network under RKP, one must compromise 230 sensors under random attack but only 160 under selective attack. Under SKRP, the attacker must compromise 200 sensors under random attack, but only 125 sensors under selective attack.

An attacker who wants to compromise links between all neighboring sensor pairs can, at each step, target the sensor s_t whose compromise reveals the largest number of unknown pairwise keys. The attacker gains all preloaded keys at s_t, *and all path keys mediated by* s_t. Let $[s_j, s_k]$ represent the path key between s_j and s_k, and let $M(s_i) = \{[s_{i_{11}}, s_{i_{12}}], [s_{i_{21}}, s_{i_{22}}], \cdots\}$ be the set of path keys mediated by s_i.

2 Modeling Selective Attack With Order Statistics

We present a novel framework, based on order statistics, for analyzing selective attacks on sensor networks. No analysis model for selective attack has appeared in the literature, since it poses major technical challenges. We have applied our framework to analyze the resilience of PIKE [12] and mGKE [13, 14].

Let $\mathcal{S} = \{s_1, s_2, \ldots, s_{n_s}\}$ be the set of sensors, and let $\mathcal{C} \subseteq \mathcal{S}$ and $\mathcal{U} \subseteq \mathcal{S}$ be the set of compromised sensors and uncompromised sensors, respectively. Initially, $\mathcal{C}$ is empty. We define the *yield* $Y_{\mathcal{C}}(s_i)$ of sensor s_i to capture how much *new* key information the compromise of s_i would reveal about the *rest* of the network, given



(a) PIKE: Marginal yield vs. κ

(b) mGKE: Marginal yield vs. κ

Figure 1: Marginal yields. κ is the number of compromises.

that the sensors in $\mathcal{C}$ have been compromised. Since all keys involving nodes in $\mathcal{C}$ are already known, we define the yield as

$$Y_{\mathcal{C}}(s_i) = M(s_i) \setminus \{[s_j, s_k] \mid s_j \in \mathcal{C} \text{ or } s_k \in \mathcal{C}\} \tag{1}$$

Under selective attack, the attacker will target the sensor s_t having the largest yield. That is, $Y_{\mathcal{C}}(s_t) = \max\{Y_{\mathcal{C}}(s_i)\}, s_i \in \mathcal{U}$. Clearly, $Y_{\mathcal{C}}(s_i)$ would be defined differently for different key establishment schemes.

2.1 Analytical and Experimental Results

Figures 1(a) and 1(b) show that the analytical and experimental values for the marginal yields under selective attack match very well. Our framework for selective attack captures its true characteristics. As expected, the marginal yield decreases with the number of compromises κ. Figure 2 compares the resilience of PIKE and mGKE under random attack (RA) and selective attack (SA). As expected, SA is more effective than RA. PIKE and mGKE exploit the uniqueness of pairwise keys, so their resilience decreases approximately linearly (sub-linearly for mGKE), with the number of compromises. In contrast [3], RKP and SRKP resilience degrades dramatically after a threshold under both random and selective attack.

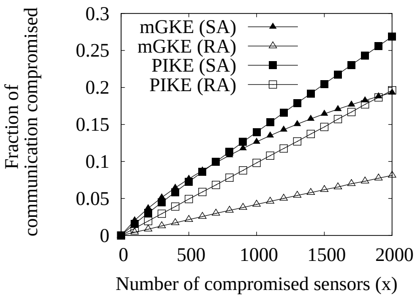


Figure 2: PIKE & mGKE resilience

3 Conclusion

Our framework based on order statistics has proved effective in analyzing the effects of selective compromises in sensor networks. No general framework for modeling selective attack has appeared in the literature, since modeling selective attack is technically challenging. The specifics of deriving the yield metric depend on the key establishment scheme. However, our analytical and experimental results match very closely for both PIKE and mGKE, demonstrating that our approach is sound and very practical.

References

[1] D. Liu and P. Ning., "Location-based pairwise key establishments of static sensor networks," in *ACM Workshop in Security in Ad Hoc and Sensor Networks*, 2003.

[2] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *INFOCOM*, 2004.

[3] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key manageent scheme for wireless sensor networks," in *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2004.

[4] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in *INFOCOM*, 2004.

[5] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks," in *IEEE Symposium on Security and Privacy*, 2004.

[6] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," in *Proceedings of the IEEE International Conference on Pervasive Services*, 2005.

[7] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM Press, 2005, pp. 34–45.

[8] L. Eschenaer and V.D.Gligor, "A key-management scheme for distributed sensor networks," in *ACM Conference on Computer and Communications security(CCS)*, 2002.

[9] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE Symposium on Security and Privacy*, 2003.

[10] W. Du, J. Deng, Y. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *ACM Conference on Computer and Communications security(CCS)*, 2003.

[11] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *ACM Conference on Computer and Communications security(CCS)*, 2003.

[12] H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," in *Infocom*, 2005.

[13] L. Zhou, J. Ni, and C. Ravishankar, "(SHORT PAPER) GKE: Efficient Group-based Key Establishment for Large Sensor Networks," in *Proceedings of the First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm'05)*, 2005.

[14] L. Zhou, J. Ni, and C. V. Ravishankar, "Efficient key establishment for group-based wireless sensor deployments," in *WiSe '05: Proceedings of the 4th ACM workshop on Wireless security*, 2005, pp. 1–10.