**Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks**

**LITERATURE SURVEY**

**A Survey on Privacy-preserving Schemes for Smart Grid Communications**

In this paper, we present a comprehensive survey of privacy-preserving schemes for Smart Grid communications. Specifically, we select and in-detail examine thirty privacy preserving schemes developed for or applied in the context of Smart Grids. Based on the communication and system models, we classify these schemes that are published between 2013 and 2016, in five categories, including, 1) Smart grid with the advanced metering infrastructure, 2) Data aggregation communications, 3) Smart grid marketing architecture, 4) Smart community of home gateways, and 5) Vehicle-to grid architecture. For each scheme, we survey the attacks of leaking privacy, countermeasures, and game theoretic approaches. In addition, we review the survey articles published in the recent years that deal with Smart Grids communications, applications, standardization, and security. Based on the current survey, several recommendations for further research are discussed at the end of this paper.

In this article, we surveyed the state-of-the-art of privacy-preserving schemes for Smart Grids, which are published between 2013 and 2016. We presented the survey articles published in the recent years that describe, namely, Smart Grid communications, Smart Grid applications, Smart Grid security, and Smart Grid privacy. We also presented the major threats of leaking privacy in Smart Grids, including, key-based attacks, data-based attacks, impersonation-based attacks, and physical-based attacks. We reviewed the countermeasures, game theoretic, and formal proof models proposed for Smart Grids used by privacy preserving schemes. We presented a side-by-side comparison in a tabular form for the current state-of-the-art of privacy-preserving schemes (thirty) proposed for Smart Grids. As we have reviewed, privacy-preserving schemes for Smart Grids have advanced significantly in recent years, especially because the need for better privacy for power industry has increased.

**On Broadcast Authentication in Wireless Sensor Networks**

Broadcast authentication is a critical security service in wireless sensor networks (WSNs), since it enables users to broadcast the WSN in an authenticated way. Symmetric key based schemes such as µTESLA and multilevel µTESLA have been proposed to provide such services for WSNs; however, these schemes all suffer from serious DoS attacks due to the delay in message authentication. This paper presents several effective public key based schemes to achieve immediate broadcast authentication and thus overcome the vulnerability presented in the µTESLA-like schemes. Several cryptographic techniques, including Merkle hash tree and identity-based signature scheme, are adopted to minimize the scheme overhead regarding the costs on both computation and communication. A quantitative energy consumption analysis of the proposed schemes is given in detail. We believe that this paper can serve as the start point towards fully solving the important multisender broadcast authentication problem in WSNs.

In this paper, we first revisited the problem of multisender broadcast authentication in WSNs. We pointed out that symmetric-key based solutions such as μTESLA are insufficient for this problem by identifying a serious security vulnerability inherent to these schemes: the delayed authentication of the messages can lead to severe DoS attacks, due to the stringent energy and bandwidth constraints in WSNs. We then came up with several effective PKC-based schemes to address the proposed problem. Both computational and communication costs are minimized. We further analyzed both the performance and security resilience of the proposed schemes. We believe that this paper can serve as the start point towards fully solving the important multisender broadcast authentication problem in WSNs.

**Industrial Automation using Internet of Things (IOT)**

Internet of Things (IoT) is rapidly increasing technology. IoT is the network of physical objects or things embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. In this paper, we are developing a system which will automatically monitor the industrial applications and generate Alerts/Alarms or take intelligent decisions using concept of IoT. IoT has given us a promising way to build powerful industrial systems and applications by using wireless devices, Android, and sensors. A main contribution of this review paper is that it summarizes uses of IoT in industries with Artificial Intelligence to monitor and control the Industry.

Nowadays we need everything computerized. Earlier we can only monitor the situations with the help of cameras. In industries to reduce manual overhead we have implemented Internet of Things (IoT) in Industry to monitor as well as to inform the responsible person to take appropriate measures, but this will partially fulfill our requirement. As sometimes it will be late in this process and it will harm to property as well as life. For this purpose we are developing a system for Industrial Automation using IoT with the help of Artificial Intelligence to make system automated which will take intelligent decisions.

**A Key-Management Scheme for Distributed Sensor Networks**

Distributed Sensor Networks (DSNs) are ad-hoc mobile networks that include sensor nodes with limited computation and communication capabilities. DSNs are dynamic in the sense that they allow addition and deletion of sensor nodes after deployment to grow the network or replace failing and unreliable nodes. DSNs may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary. Hence DSNs require cryptographic protection of communications, sensor capture detection, key revocation and sensor disabling. In this paper, we present a key-management scheme designed to satisfy both operational and security requirements of DSNs. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared-key discovery and path-key establishment, and for key revocation, re-keying, and incremental addition of nodes. The security and network connectivity characteristics supported by the key-management scheme are discussed and simulation experiments presented.

We presented a new key management scheme for largescale DSNs. All such schemes must be extremely simple given the sensor-node computation and communication limitations. Our approach is also scalable and flexible: trade-offs can be made between sensor-memory cost and connectivity, and design parameters can be adapted to fit the operational requirements of a particular environment. We illustrated the effect of modifying design parameters using both analysis and simulations. The results indicate that our scheme is superior to the traditional key pre-distribution schemes.

**A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge**

To achieve security in wireless sensor networks, it is important to be able to encrypt messages sent among sensor nodes. Keys for encryption purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. Recently, a random key predistribution scheme and its improvements have been proposed. A common assumption made by these random key predistribution schemes is that no deployment knowledge is available. Noticing that in many practical scenarios, certain deployment knowledge may be available a priori, we propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. We show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can be substantially improved with the use of our proposed scheme. The scheme and its detailed performance evaluation are presented in this paper.

We have described a random key pre-distribution scheme that uses deployment knowledge. With such knowledge, each node only needs to carry a fraction of the keys required by the other key pre-distribution schemes while achieving the same level of connectivity. The reduction in memory usage not only relieves the memory requirement on the memory constrained sensor node, but more importantly, it substantially improves network’s resilience against node capture. We have shown these improvements using our analytical and simulation results.

**Insider Threats in Wireless Sensor Networks and Their Countermeasures**

Wireless sensor networks tend to have a wide range of applications in our day to day life. In future, they can be used to survey our health, our home, the roads we follow, the office or the industry we work in or even the aircrafts we use, in an attempt to enhance our safety. But, these networks themselves are prone to security attacks. The list of security attacks is already very large and keeps on increasing with the expansion of these networks. A powerful tool for the detection of faulty or malicious nodes is the trust management schemes. Having detected the misbehaving nodes, their neighbours can use this information to avoid relying on them, either for data forwarding, data aggregation or any other cooperative function. There are a variety of trust models and most of them focus on defending against certain insider attacks. This paper discusses several security vulnerabilities that the trust mechanisms have. We also examine how inside attackers can exploit these security holes, and propose approaches that can mitigate the weaknesses of trust mechanisms.

In this paper, we discussed the serious threats that insider attacks pose to WSNs even with the presence of trust mechanism and watchdog. We also discussed defending approaches for improving trust mechanism to counter these insider attacks. In the near future, we can design a reliable, energy-efficient trust mechanism for WSNs by considering the identified vulnerabilities and defending approaches.

**MCRT: Multi-Channel Real-Time Communications in Wireless Sensor Networks**

As many radio chips used in today’s sensor mote hardware can work at different frequencies, several multi-channel communication protocols have recently been proposed to improve network throughput and reduce packet loss for wireless sensor networks. However, existing work cannot utilize multiple channels to provide explicit guarantees for application-specified end-to-end communication delays, which are critical to many real-time applications such as surveillance and disaster response. In this paper, we propose MCRT, a multi-channel real-time communication protocol that features a flow-based channel allocation strategy. Because of the small number of orthogonal channels available in current mote hardware, MCRT allocates channels to network partitions formed based on many-to-one data flows. To achieve bounded end-to-end communication delay for every data flow, the channel allocation problem has been formulated as a constrained optimization problem and proven to be NP-complete. We then present the design of MCRT, which includes a channel allocation algorithm and a real-time packet forwarding strategy. Extensive simulation results based on a realistic radio model and empirical results on a real hardware testbed of Tmote nodes both demonstrate that MCRT can effectively utilize multiple channels to reduce the number of deadlines missed in end-to-end communications. Our results also show that MCRT outperforms a state-of-the-art real-time protocol and two baseline multi-channel communication schemes.

Multi-channel communications have recently shown great promise to improve network throughput and reduce packet loss for wireless sensor networks. However, existing research does not utilize multiple channels to provide explicit guarantees for application-specified end-to-end communication delays, which are critical to many real-time applications such as surveillance and disaster response. In this paper, we have presented MCRT, a multi-channel real-time communication protocol that utilizes both multiple channels and transmission power adaptation to achieve real-time communications in WSNs. MCRT features a flow-based channel allocation strategy, which is designed based on the multi-channel realities identified in previous work to use only a small number of orthogonal channels. To achieve bounded end-to-end communication delay for every data flow, the channel allocation problem has been formulated as a constrained optimization problem and proven to be NP-complete. The design of MCRT includes a channel allocation algorithm designed based on well-established heuristics and a real-time packet forwarding strategy. Extensive simulation results and empirical results on real hardware testbed of Tmote nodes both demonstrate that MCRT can effectively utilize multiple channels to reduce the number of deadlines missed in end-to-end communications. Our results also show that MCRT outperforms a state-of-the-art real-time protocol and two baseline multi-channel communication schemes.

**Location-Based Pairwise Key Establishments for Static Sensor Networks**

Sensor networks are ideal candidates for applications such as target tracking and environment monitoring. Security in sensor networks is critical when there are potential adversaries. Establishment of pairwise keys is a fundamental security service, which forms the basis of other security services such as authentication and encryption. However, establishing pairwise keys in sensor networks is not a trivial task, particularly due to the resource constraints on sensors. This paper presents several techniques for establishing pairwise keys in static sensor networks. These techniques take advantage of the observation that in static sensor networks, although it is difficult to precisely pinpoint sensors’ positions, it is often possible to approximately determine their locations. This paper presents a simple location-aware deployment model, and develops two pairwise key predistribution schemes, a closest pairwise keys predistribution scheme and a location-based pairwise keys scheme using bivariate polynomials, by taking advantage of sensors’ expected locations. The analysis in this paper indicates that these schemes can achieve better performance if such location information is available and that the smaller the deployment error (i.e., the difference between a sensor’s actual location and its expected location) is, the better performance they can achieve.

In this paper, we presented two schemes to take advantage of sensors’ location information, aiming at improving pairwise key establishment in sensor networks. When sensors in a network can be deployed to the expected locations with a certain precision, our schemes provide better security and performance over the previous solutions. Our first scheme, the closest pairwise keys scheme, is resistant to node capture attacks and has no limit on the total number of sensors. Its extended version further reduces the storage overhead and simplifies the dynamic deployment of new sensors. Our second scheme, the location-based key predistribution using bivariate polynomials, employs a threshold technique and provides a trade-off between the security against node capture and the performance of establishing pairwise keys.

**Distributed Detection of Node Replication Attacks in Sensor Networks**

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties [17], i.e., properties that arise only through the collective action of multiple nodes. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and Line-Selected Multicast displays particularly strong performance characteristics. We show that emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

We have discussed various approaches used to detect node replication. In Section 3, we show how centralized approaches place excessive trust in the base station and excessive load on those nodes near it. Local voting schemes are ill equipped to detect distributed node replication. In contrast, we present two schemes that enable distributed detection of distributed events. The final scheme, Line-Selected Multicast, provides excellent resiliency while achieving near optimal communication overhead with only modest memory requirements. Both of our primary schemes illustrate the power of emergent properties in sensor networks. Given the adversary model typically assumed in sensor networks, we argue that the security of such networks will increasingly depend on emergent algorithms. Cost considerations and unattended deployment will always leave individual sensors vulnerable to compromise. Since we cannot predict the exact nature or number of targets the adversary will select, the network must collectively resist, report and revoke compromised nodes in a manner that goes beyond traditional intrusion detection systems. We expect that emergent algorithms will ultimately provide the best defense against these insidious attacks.