© 2012 **DSRC**

PERFORMANCE ENHANCEMENT USING AUTHENTICATED DATA FILTRATION IN WIRELESS NETWORK A RELIABILITY PERSPECTIVE

Arun Patnaik.P[1*], D.Srinivas[2*], K.Ravi kumar[3*]

1. *M.Tech (CSE) Student, Department of CSE, KIET, Korangi, Dist: E. Godavari, A.P, India*
2. *Asst. Prof, Department of CSE, KIET, Korangi, Dist: E. Godavari, A.P, India*
3. *Asst. Prof, Department of CSE, KIET, Korangi, Dist: E. Godavari, A.P, India*

Keywords:
Performance and network Security, Quality of Service (QoS), Key management, Data Filtration

Abstract: *As of the technology is advancing, Wireless Sensor Networks (WSNs) are gradually adopted in the industrial world due to their advantages over wired networks. In addition to saving cabling costs, WSNs widen the realm of environments feasible for monitoring. They thus add sensing and acting capabilities to objects in the physical world and allow for communication among these objects or with services in the future Internet. However, the acceptance of WSNs by the industrial automation community is impeded by open issues, such as security guarantees and provision of Quality of Service (QoS). In this paper, to examine both of these perspectives, we select and survey relevant WSN technologies dedicated to industrial automation. We determine QoS requirements and carry out a threat analysis, which act as basis of our evaluation of the current state-of-the-art. According to the results of this evaluation, we identify the security, filtration of vulnerable data. Hence, we tries give focus on efficient filtration of data using the key management mechanism.*

1. INTRODUCTION

This global market totally depend on the internet network, hence of many technology has come into existence to facilitate such service, one of them is Wireless sensor networks may be deployed in uncontrolled or even hostile environments and hence are subject to various attacks. For example, an adversary can easily gain access to mission critical information by monitoring wireless communication among sensor nodes, or inject false messages into the networks through some compromised nodes. Therefore, it is crucial to deploy secret keys into wireless sensor networks to encrypt wireless communication or establish authentication among sensor nodes. The challenge is how to efficiently generate, distribute and maintain secret keys among sensor nodes. This problem is called key management problem for wireless sensor networks and can be solved by carefully designed key management schemes. In this work, we survey existing key management schemes for wireless sensor networks and provide taxonomy of them. Most of schemes deal with symmetric key management, while a few of them discuss public key management. Since public key algorithms are generally considered too expensive for the use in wireless sensor networks, we focus our discussion on symmetric key management schemes. We divide these schemes into pair wise key, group key and global key schemes depending on what kind of keys they distribute and manage, and category them into probabilistic, deterministic and hybrid depending on how possible the keys can be generated. We also classify these schemes depending on whether they exploit deployment

**** Arun Patnaik.P***
M.Tech (CSE) Student, Department of CSE, KIET, Korangi, Dist: E. Godavari, A.P, India

knowledge or not. In the rest of this section, we introduce threat model and goals of key management schemes, and then discuss the pair wise key schemes, the group key schemes and a global key scheme.

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate unfettered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Node management using the high filtration mechanism or algorithms is to facilitate unrelated data.

2. RELATED WORK

There are many definitions of what constitutes application security. Many industry sources utilize the application lifecycle approach that emphasizes application fortification throughout the design, development, deployment, upgrade, and maintenance phases. Considering the facts, Sensor nodes are not tamper-resistant; hence, the adversaries can easily compromise some nodes and launch various attacks through the compromised nodes. They can inject false data into the networks. These attacks not only cause false alarms in the base station, but also consume up the limited energy of forwarding nodes. Moreover, the adversaries can launch DoS attacks by selectively dropping some forwarding data, or intentionally contaminating the authentication information of data to make it dropped by other benign nodes if some authentication mechanisms are enforced.

Wireless networks are vulnerable to various malicious attacks. We list some possible attacks as follows:

Eavesdropping: The adversaries may obtain critical or sensitive information by eavesdropping on wireless communication. Jamming: The adversaries can broadcast a high-power signal to disrupt or interfere with wireless communication. Replaying: The adversaries may replay the previously received messages to disturb the functionalities of wireless networks.

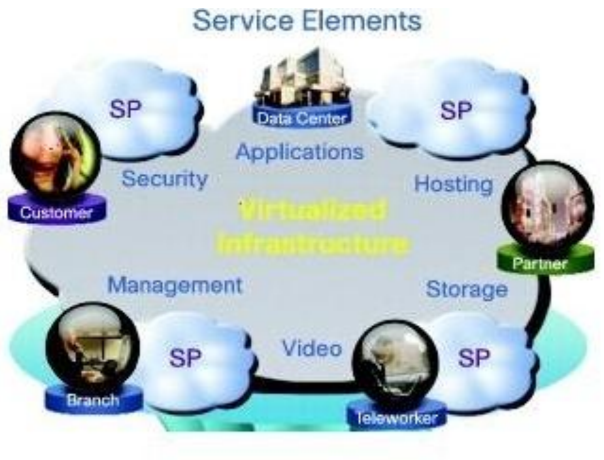

Fig. 2.1 Structural service elements in the cyclic phase of network sensor

Wormhole: The adversaries can record the information received at one location and replay them at another location via some wormhole tunnel, e.g., a fast wired link, which fools the wireless nodes far from each other to believe they are neighbors. Dropping/Selective Forwarding: The adversaries may compromise some nodes, and drop all or some of the messages that should be forwarded by those nodes. Flooding: The adversaries may inject a huge amount of useless information into wireless networks via some compromised nodes to disrupt wireless communication and/or deplete the energy of wireless nodes. Modification/Pollution: The adversaries can modify or corrupt the information transmitted in wireless networks.

False Data Injection: The adversaries can inject false information into wireless networks to disturb the functionalities of wireless networks and/or deplete the energy of wireless nodes. Impersonating/Sybil Attack: A compromised node can impersonate another legal node or claim the identities of multiple legal nodes. Inductive key derivation is the process of deriving a key by coercing information from the wireless LAN and is also referred to as an active network attack. As mentioned in the section on stream ciphers, encryption is accomplished by performing the XOR function with the stream cipher to produce the cipher-text. Inductive network attacks work on this premise. Network-based services and managed services in general introduce more stringent requirements for application security, thereby creating an internal demand for the customer-facing service. For securing data and applications in a virtualized or multi-tenant environment, service providers must rely on federated identity capabilities. Consider the following services, capabilities, and deployment models that require application security built into the service delivery model itself:

3. METHODS

Regardless of technology related to networking, Wireless communication is prone to eavesdropping. In wireless sensor networks, distributing secret keys among sensor nodes allows them to secure their communication with encryption. Key management, including key generation, distribution, revocation and update, not only provides the basic cryptographic service, but also are critical to implement other security mechanisms. However, there are still a lot of unsolved problems in providing efficient key management for wireless sensor networks. For example, sensor nodes may not have sufficed memory for key storage and cannot support heavy public-key algorithms. These problems motivate us to study key management for wireless sensor networks. In this paper, we identify three aspects related to the context.

I. Key management for wireless sensor networks between sensor nodes should be secured, which demands the efficient distribution of secret keys. Key management provides not only the fundamental cryptographic services, but also the basic component to construct other security mechanisms, hence, should be carefully studied.

II. Filtering false data injection and DoS attacks in wireless sensor networks (for authenticity and availability). For various applications to function correctly, it is important to make sure that valid information can be delivered to desired destinations. However, false data injection produces invalid information and DoS attacks disrupt information delivery. So, they must be efficiently filtered.

III. Secure network coding (for integrity). Network coding is promising to maximize network throughput and gains more and more applications in wireless networks. However, it poses a lot of new security problems that have not been well addressed. As of we come across the filtration mechanism to vulnerable data discussed in the section.2. It follows following steps:

Secure connectivity: These features provide highly secure and scalable network connectivity, incorporating multiple types of traffic. Examples include IP Security (IPSec) VPN, Group Encrypted Transport VPN, Dynamic Multipoint VPN, Enhanced Easy VPN, and Secure Sockets Layer (SSL) VPN. Typical IP networks run innumerable applications, both legitimate and surreptitious, that compete with voice, video and real-time data applications that are sensitive to performance. For example, voice traffic is sensitive to latency-voice packets are typically smaller and if they are queued behind large noncritical data packets, you can immediately perceive the degradation as audible clicks. Video traffic consumes high bandwidth and is sensitive to jitter; it is often impractical to buffer video data during delays, so packets are usually dropped with a view to quickly returning to a steady stream; if this packet loss happens too often, the result is a choppy stream and unhappy viewers.

These enterprise voice and video applications require sophisticated quality of service (QoS) and IP Multicast mechanisms to preserve voice and video quality. The premise of site-to-site and remote-access VPNs is to transport this traffic mix over encrypted ubiquitous and inexpensive public Internet access, for both primary and backup connectivity. Extending voice and video application quality over VPNs brings additional requirements in the form of integration of IPSec with QoS or IP Multicast. Voice over IP and IPTV are already mainstream; systems continue to grow in adoption. As these real-time voice and video telephony applications proliferate, so too do the VPN and security performance, scale, and feature integration requirements at the branch-office site. It leads to sometimes the filtration mechanism to so complex; hence every packet has to filter in the sense of network.

QoS: Low-Latency Queuing (LLQ) before cryptography is a critical requirement to help ensure voice quality over VPNs. The embedded processor provides LLQ as well as post encryption interface-level QoS.

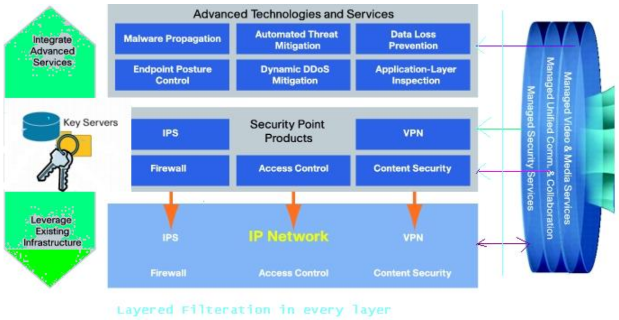
Advanced Technologies and Services
Malware Propagation
Automated Threat Mitigation
Data Loss Prevention
Endpoint Posture Control
Dynamic DDoS Mitigation
Application-Layer Inspection
Integrate Advanced Services
Key Servers
IPS
Security Point Products
VPN
Firewall
Access Control
Content Security
Leverage Existing Infrastructure
IPS
IP Network
VPN
Firewall
Access Control
Content Security
Managed Video & Media Services
Managed Unified Comm. & Collaboration
Managed Security Services
Layered Filteration in every layer

Fig.3.1 Architecture of Filtration of vulnerable data

IP Multicast : Secure Multicast is a foundational technology that combines the keying protocol, Group Domain of Interpretation (GDOI) with IPSec encryption to provide users an efficient method to secure IP Multicast traffic. It enables the router to apply encryption to no tunneled (that is, "native") IP Multicast packets, increasing efficiency by eliminating the requirement to configure separate tunnels. Encapsulating IP Multicast packets allows IP Multicast routing (for example, Protocol Independent Multicast (PIM)) to route the packets even though they are encrypted. Native IP Multicast encapsulation also avoids the excessive packet replication that normally occurs with unicast tunnels. Secure Multicast is well suited for applications such as encryption of IP packets sent over satellite links, encryption in audio conferencing, secure real-time content replication, and DMVPN, among others.

Integrated threat control: These features prevent and respond to network attacks and threats using network services. Examples include Cisco IOS® Firewall, Cisco IOS Intrusion Prevention System (IPS), Content Filtering, NetFlow, and Flexible Packet Matching (FPM).

Trust and identity: These features allow the network to intelligently protect endpoints using technologies such as authentication, authorization, and accounting and public key infrastructure (PKI). Shared key authentication requires the client use a pre shared WEP key to encrypt challenge text sent from the access point. The access point authenticates the client by decrypting the shared key response and validating that the challenge text is the same. The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack. An eavesdropper can capture both the plain-text challenge text and the cipher-text response. WEP encryption is done by performing an exclusive OR (XOR) function on the plain-text with the key stream to produce the cipher-text. It is important to note that if the XOR function is performed on the plain-text and cipher-text the result is the key stream leads to high level of sensory.

4. CONCLUSION

Application security is not a standalone security requirement. Rather, it must be addressed across business networks and, more importantly, across business processes. It should be regarded as part of the broader set of business requirements for minimizing business risk, maximizing employee productivity, and protecting company brands and corporate reputations. Wireless sensor networks support various applications such as battlefield surveillance, target tracking or traffic control, in which sensor nodes should report detected events or sensing readings to the base station. However, the data reports are vulnerable to forging, modifying and dropping and the adversaries can inject false data into networks. The forged reports about battlefield may cause false alarms in the base station and the dropped reports might be critical for traffic control. So, it is important to ensure that the information transmitted with wireless sensor networks is valid, correct and available. Some solutions for filtering false data injection are not efficient and robust for dynamic sensor networks, while few of them consider DoS attacks simultaneously. Thus, we are inspired to address both attacks for wireless sensor networks. Hence for further analysis of the performance we may have to extend the reliability.

5. REFERENCE

[1] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient security mechanisms for large-scale distributed sensor networks,” in *Proc. ACM CCS*, 2003, pp. 62–72.

[2] http://dl.acm.org/citation.cfm?id=1086505

[3] S. Capkun and J. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in Proc. IEEE INFOCOM, 2005, vol. 3, pp. 1917–1928.

[4] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. ACM CCS, 2002, pp. 41–47.

[5] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, “Rangefree localization schemes in large scale sensor network,” in Proc. ACM MobiCom, 2003, pp. 81–95.

[6] C. karlof and D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” in Proc. 1st IEEE Int. Workshop Sensor Network Protocols Appl., 2003, pp. 113–127.

[7] B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in Proc. ACM MobiCom, 2000, pp. 243–254.

[8] L. Lazos and R. Poovendran, “SeRLoc: Secure range-independent localization for Wireless sensor networks,” in Proc. ACMWiSe, 2004, pp. 21–30.

[9] L. Lazos, R. Poovendran, and S. Capkun, “ROPE: Robust position estimation in wireless sensor networks,” in Proc. IPSN, 2005, pp. 324–331.

[10] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in Proc. ACM CCS, 2003, pp. 52–56.

[11] R. Nagpal, H. Shrobe, and J. Bachrach, “Organizing a global coordinate system from local information on an ad hoc sensor network,” in Proc. IPSN, 2003, LNCS 2634, pp. 333–348.

[12] D. Nicolescu and B. Nath, “Ad-hoc positioning systems (APS),” in Proc. IEEE GLOBECOM, 2001, vol. 5, pp. 2926–2931.

[13] A. Perrig, R. Szewczyk, V. Wen, D. Culer, and J. Tygar, “SPINS: Security protocols for sensor networks,” in Proc. ACM MobiCom, 2001, pp. 189–199.

[14] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure information aggregation in sensor networks,” in Proc. ACM SenSys, 2003, pp. 255–265.

[15] K. Ren, W. Lou, and Y. Zhang, “LEDS: Providing location-aware end-to-end data security in wireless sensor networks,” in Proc. IEEE INFOCOM, 2006, pp. 1–12.

[16] “TinyOS community forum,” [Online]. Available: http://www. tinyos.net

[17] A.Woo, T. Tong, and D. Culler, “Taming the underlying challenges of reliable multihop routing in sensor networks,” in Proc. ACM SenSys, 2003, pp. 14–27.

[18] H. Yang and S. Lu, “Commutative cipher based en-route filtering in wireless sensor networks,” in Proc. IEEE VTC, 2004, vol. 2, pp. 1223–1227.

[19] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward resilient security in wireless sensor networks,” in Proc. ACM MobiHoc, 2005, pp. 34–45.

[20] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route detection and filtering of injected false data in sensor networks,” in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446–2457.

[21] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks,” Comput. Sci. Dept., Univ. California, Los Angeles, UCLA-CSD TR-01–0023, 2001.