Research Inventy: International Journal of Engineering And Science
Vol.12, Issue 7 (July 2022), PP 13-20
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Wireless and Mobile Security

Tapan Golakiya
Software Development Engineer, Brillio LLC, Canton, MI, USA
Corresponding Author: golakiyatapan@gmail.com

Abstract: *Wireless and Mobile Security is a study of the security of wireless networks and mobile devices. In this report, we discuss different wireless protocols and look at methods to secure them. We also look at the security concerns in mobile devices and mobile applications. Then we discuss different Wireless security protocols, problems with them and solutions. The study includes attacks against the Wired Equivalent Privacy protocol for wireless networks.*

Keywords: *dimensionality, variance, correlation, K-means, clustering..*

Date of Submission: 20-02-2021 Date of Acceptance: 10-03-2021

1. INTRODUCTION

In recent years, the use of laptop computers and other mobile devices has caused an increase in the range of places people perform computing. At the same time, wireless network connectivity is becoming an important part of computing environments. As a result, wireless networks of various kinds have gained much popularity and is growing at much higher rate. But with the convenience of wireless access come some new problems, from which many problems are related to the security concerns. As the wireless network is open to all, there are many kinds of threats to this system. In this report we will discuss different wireless protocols which are used for wireless communications, explore their weaknesses, and look at methods to secure them. Also, look at the security that can be used in the mobile devices and mobile applications also, learn about how certain techniques will help to make this device more secure and long lasting.

2. TECHNICAL OVERVIEW

In the wireless network system different protocols are used to enable communication between different devices. The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, we will discuss several serious security flaws in the protocol and the attacks that might take place due to this flaw. [1] We will also discuss some attacks against WEP, the link- layer security protocol for 802.11 networks. In this we will see how we are able to recover the 128-bit secret key used in a production network, with a passive attack. [2]

Mobile sinks are important in most of the wireless sensor network applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. But, in a sensor network where we make use of existing key pre-distribution schemes for pairwise key establishment and authentication between sensor nodes and mobile sinks, we face a new security challenge and that is that in the basic probabilistic and q-composite key pre-distribution schemes, an attacker can easily obtain many keys by capturing a small fraction of nodes. Here we will discuss the three-tier general framework which will allow the use of any pairwise key pre-distribution scheme as its basic component. Now to avoid this kind of attack we make use of framework with two separate key pools, one for the mobile sink to access the network, and one for pairwise key establishment between the sensors. [6]

Wireless Sensor Networks they are very much subjected to the security threats. To add security, we need more energy, and this may reduce the lifetime of the sensor nodes. To avoid this, the concept of Middleware is introduced. Middleware provides security for the Wireless Sensor Networks in the Mobile agent and has capability of optimizing the power usage with the sensor nodes. We will also discuss security concerns in mobile appliances, and study the challenges that confront system architects, Hardware engineers, and Software developers, also, see how we can bridge the processing and battery gaps, efficient tamper-proofing of devices, content protection, etc.

3. DISCUSSION: WIRELESS AND MOBILE SECURITY

In this section we will discuss in detail the topics under wireless and Mobile Security.

A. Wired Equivalent Privacy (WEP Protocol)

In 802.11 networks, the Wired Equivalent Privacy protocol is used to protect link-level data during wireless transmission. WEP protocol relies on a secret key k shared between the communicating parties to protect the content of a transmitted data. It is protected by using encryption as following:

- ***Checksumming***: First, we find out integrity checksum c(M) on the message M. We concatenate the two to obtain a plaintext P = (M, c(M)), which we can use as an input to the second stage. Note that c(M), and thus P, does not depend on the key k.
- ***Encryption:*** We encrypt the plaintext P derived above using RC4. We then choose an initialization vector (IV) v. Here, the RC4 algorithm generates a keystream as a function of the IV v and the key k. This keystream is denoted by RC4(v,k). Then, we exclusive-or (XOR) the plaintext with the keystream to obtain the ciphertext:

$$C=P \oplus RC4(v,k).$$

- ***Transmission:*** Finally, we transmit the IV and the ciphertext over the radio link. Symbolically, this may be represented as follows:

$$A \text{ -> } B : v,(P \oplus RC4(v,k)) \text{ Where } P = (M, c(M))$$

Figure 1: [1]. To decrypt a frame protected by WEP, the recipient simply reverses the encryption process. This time first, we regenerate the keystream and XORs it against the ciphertext to recover the initial plaintext. [1]

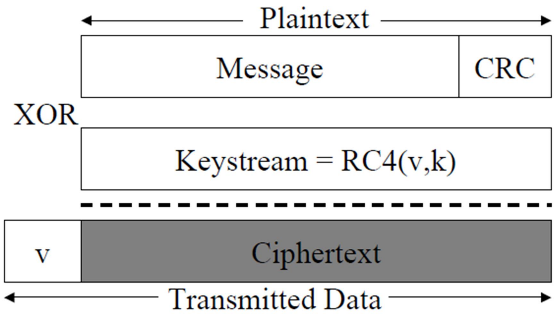


Figure 1: WEP Encryption Frame [1]

The security goals of this protocol are:

- ***Confidentiality***: The fundamental goal of WEP is to avoid eavesdropping.
- ***Access control:*** Protect access to a wireless network infrastructure. The 802.11 standard includes feature that can block all packets that are not properly encrypted using WEP to provide access control.
- ***Data Integrity:*** A related goal is to prevent tampering with transmitted messages. [1]

1) ***Problems With WEP:*** WEP does not meet its fundamental goals of wired-equivalent confidentiality. WEP also fails to meet the expected goals for integrity and authentication. The two generic limitations are: The first one is, use of WEP is optional, and as a result, many real installations never even turn on encryption. This is unfortunate, as it does not matter how good the cryptography is if it is never used and the second one is, by default, WEP uses a single shared key common to all users of a WLAN, and this common key is often stored in software-accessible storage on each device. If any device is lost, stolen, or compromised, the only recourse is to change the shared secret in all the remaining devices. Since WEP does not include a key management protocol, distributing the new secret to all users is an unwieldy process. As a result, key compromises are often ignored. Regardless of the cryptography employed, these shortcomings make it difficult to obtain confidentiality and integrity in WLAN deployments. The most serious problem with WEP is its encryption keys can be recovered through cryptanalysis. WEP uses a common stream cipher, RC4, but in a nonstandard way: WEP concatenates a base key with a 24-bit per-packet nonce, called the WEP Initialization Vector (IV), and uses the result as a prepacked RC4 key. In August 2001, Fluhrer, Mantin, and Shamir [4] described a stunning new attack on this construction. They showed that an eavesdropper who can obtain several million encrypted packets whose first byte of plaintext is known can deduce the base RC4 key by exploiting properties of the RC4 key schedule. Within a week, Stubblefield, Ioannidis, and Rubin experimentally implemented the attack, and demonstrated that real systems could be cracked [10]. The first octet encrypted under WEP is a known fixed value, and they found that the required ciphertext packets can be readily obtained after eavesdropping on a network for a few hours. Since then, others implemented the Fluhrer- Mantin-Shamir (FMS) attack and publicly released tools automating the process of breaking into WEP-protected networks. Because the attack uses off the-shelf hardware and software, it is a serious threat. [3]

2) ***Long-Term Solution:*** In Counter-Mode-CBC-MAC (CCMP) Protocol, the long-term solution addresses all known WEP deficiencies, but without the shackles of already-deployed hardware. The Advanced Encryption System (AES) was selected for the encryption algorithm. Mode of Operation. None of the existing AES modes of operation offers a suitable balance of features required by this application. The following features are desirable:

- Use a single key to provide confidentiality and integrity, to reduce key management overhead and minimize the time spent computing AES key schedules.
- Provide integrity protection for the plaintext packet header, as well as integrity and confidentiality of the packet payload.
- Allow precomputation to reduce latency. Since packets can be lost, the receiver may perform precomputation for a packet that never arrives. However, the sender's efforts are rarely discarded.
- Support pipelining to increase throughput.
- Small implementation size, to keep costs reasonable.
- Small overhead for each packet.
- Avoid modes that are encumbered by patents (or pending patents). A new mode called CCM was designed to meet all these criteria. CCM merges two well-known and widely deployed techniques. CCM uses counter mode for encryption and the Cipher Block Chaining Message Authentication Code (CBC-MAC) [9] for integrity protection. Both algorithms employ only the encryption primitive at both the sender and the receiver. CCM has been submitted to NIST for consideration as a Federal Information Processing Standard. CCM uses the same key for both confidentiality and integrity. This is normally a dangerous practice, but CCM avoids the pitfalls of this usage by guaranteeing that the space for the counter mode never overlaps with that used by the CBC-MAC initialization vector. The intuition behind CCM mode is that if AES behaves like a pseudo-random permutation, then the output of the cipher operating on each of these two spaces will be independent. The CCMP Protocol. The protocol using CCM has many properties in common with TKIP.

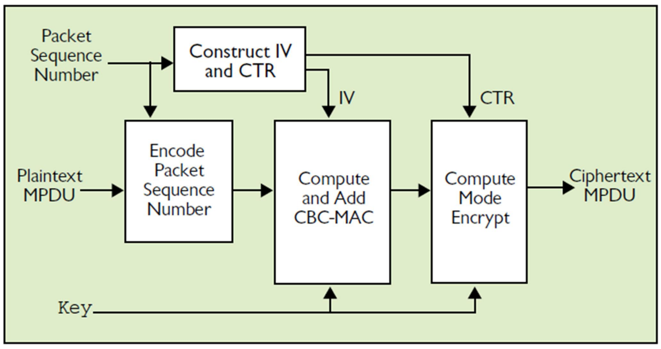


Figure 2: CCM Mode [2]

- Freedom from constraints associated with current hardware leads to a more elegant solution. Figure 2 [3] illustrates the use of CCM for a single WLAN packet fragment (MPDU). As with TKIP, CCMP employs a 48-bit IV, ensuring the lifetime of the AES key is longer than any possible association. In this way, key management can be confined to the beginning of an association and ignored for its lifetime. CCMP uses a 48-bit IV as a sequence number to provide replay detection, just like TKIP. AES has significantly different properties from the RC4 encryption algorithm used by WEP and TKIP. AES obviates any need for per-packet keys, so CCMP has no per-packet key derivation function. CCMP uses the same AES key (and associated AES key schedule) to provide confidentiality and integrity protection for all the packets in an association. The CCM MIC length is adjustable between two octets and sixteen octets. CCMP uses an 8-octet MIC, which is significantly stronger than Michael. Unlike TKIP and WEP, the encrypted ICV is no longer required. TKIP provides integrity protection over the whole MSDU and confidentiality over MSDU, leading to implementation complexity. Since CCM provides both services, it is straightforward to provide confidentiality and integrity protection over the same data structure. CCMP must, however, protect nearly the entire packet header to defend against fragmentation attacks. [2]

*3) **Wireless LAN Problems:*** Goals of the current WLAN standard was to provide security and privacy, and to meet this goal the designers implemented several security mechanisms to provide for confidentiality authentication, and access control. These mechanisms were demonstrably broken. An essential element in any security architecture is a robust and non- malleable identity. Without a reliable form of identity, malicious outsiders can potentially masquerade as valid users. In WLANs, the MAC address of the WLAN card is used as the only form of identity for both devices and users. In the early versions of the device drivers for WLAN cards, the MAC address was not changeable by the user. But here we can see, most open-source device drivers now allow the user to change the MAC address. Access Control. Access control is the process that limits those that can utilize a system resource. As such, a good access control mechanism is like a reliable doorman who only lets the occupants into a building, preventing all others from entering. There are two major forms of access control used in current WLAN equipment: access control lists, and a proprietary "closed network" mechanism. While the WLAN standard does not include an access control mechanism, most vendors have embraced the use of a MAC-address-based access control list (ACL). An ACL is essentially a lookup table based on the identity (in this case the MAC address) that indicates what resources the specific identity is permitted to use. In a WLAN, the only resource is use of the network. Thus, the MAC ACL lists the MAC addresses with permission to use the network. If the MAC address does not appear in the list, then the unlisted station is not permitted to use the network. This is one of the places where a malleable identity creates a problem. Since the MAC address can be changed at will, an attacker need only eavesdrop or sniff the wireless network to identify those

MAC addresses that are permitted access (the MAC address is always transmitted in an unencrypted form, even if WEP is used). Once an authorized MAC address is identified, the attacker needs simply change their card to the same address—now the attacker's traffic will be permitted by the ACL of the access point. The second form of widely used access control is the "closed network" approach. In this case, the user must present a secret to the access point to gain access—generally a reasonable method of access control—provided the secret remains so. Unfortunately, in the closed network approach, this is not the case. The string used as the shared secret is the BSS or network name, and this name is broadcast in the clear in several management frames during normal WLAN operation. As a result, once again the attacker need only "sniff" the network to gain enough information to use the network resources. Note that even disabling the broadcasting of the network name in the "beacon" management frame does not prevent an adversary from learning the network name as it also appears in the "probe request" and "probe response" management frames. Authentication. The current WLAN standard includes two forms of authentication: open system and shared key. The open system authentication is a null authentication process where the station, or client, always successfully authenticates with the access point, that is, the access point permits everyone to authenticate successfully. The second authentication method utilizes a shared key with a challenge and a response. The authentication process uses four messages as shown in Figure 3. [3]

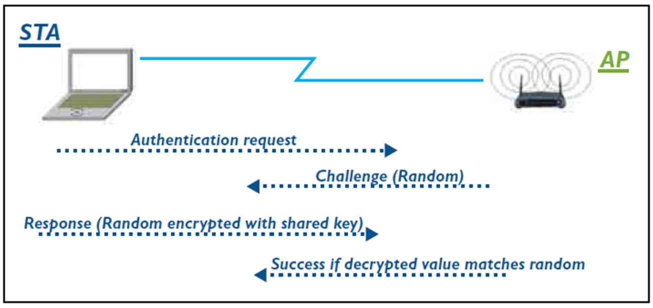
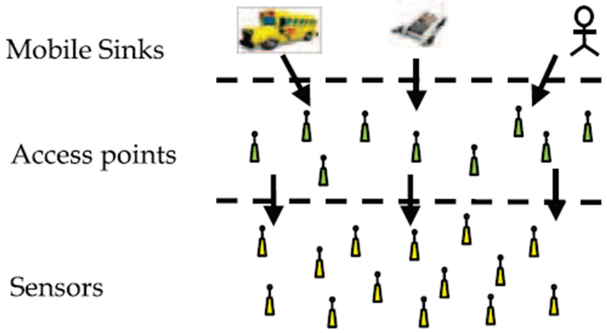

STA
AP
Authentication request
Challenge (Random)
Response (Random encrypted with shared key)
Success if decrypted value matches random

Figure 3: Shared Key Authentication. [3]

B. *Wireless Sensor Network (WSN)*

In this section we are going to discuss some of the issues that the WSN come across:

*1) **The Three-Tier Security Scheme in Wireless Sensor Networks:*** The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks: Wireless sensor networks (WSNs) consisting of many low-power, low-cost sensor nodes that communicate wirelessly. The sensed data often need to be sent back to the base station for analysis. However, when the sensing field is too far from the base station, transmitting the data over long distances using multi-hops may weaken the security strength are essential components in the operation of many sensor network applications, including data collection in hazardous environments, localized reprogramming, oceanographic data collection, and military navigation. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key pre-distribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks. However, the problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. To address the above- mentioned problem, we have developed a general framework that permits the use of any pairwise key pre-distribution scheme as its basic component, to provide authentication and pairwise key establishment between sensor nodes and MSS. To facilitate the study of a new security technique, we first cultivated a general three-tier security framework for authentication and pairwise key establishment, based on the polynomial pool-based key pre-distribution scheme. The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution approach, as an attacker would have to compromise many more sensor nodes to launch a successful mobile sink replication attack. In the new security framework, a small fraction of the preselected sensor nodes (see Fig. 1).



A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes. Rather, the attacker would also have to capture sensor nodes that carry keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain access to the network for data gathering. Although the above security approach makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution scheme, it is still vulnerable to stationary access node replication attacks. In these types of attacks, the attacker can launch a replication attack like the mobile sink replication attack. [8]

2) ***Different Environments for Wireless Security Network deployments:*** WSNs have been deployed in different environments, including disaster relief operations, seismic data collection, monitoring wildlife and battlefield management/military intelligence. Sensors can be installed in a variety of environments and usually establish a wireless network infrastructure to communicate and exchange information into their operating area. The sensor node is characterized by limited computing power and hence has a low price. Due to their small size, sensors can be spatially scattered to form an ad hoc network. Therefore, WSNs require an appropriate cryptosystem to ensure secure communication and mutual trust between their component nodes. In this scenario, key management becomes an issue of paramount importance since most of the encryption-related primitives require the use and distribution of keys in their operations. In many of these applications, sensor nodes transmit critical information over the network; therefore, security services, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key pre-distribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks. However, the problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks.
The symmetric-key based approach requires complex key management, lacks scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key whereas the shared key is used by the sender to generate a message authentication code (MAC) for each transmitted message.[6]

*3) **Middleware Security for Wireless Sensor Networks:*** A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate to achieve a common goal. A WSN can be deployed in harsh environments to fulfil both military and civil applications. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. Sensor nodes are vulnerable to security threats, so it is essential to provide immunity to the system. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. Mobile agents roam among nodes and have the properties of autonomy and cooperation. These mobile agents need a platform to work on top of sensor nodes operating system. A well-designed middleware can potentially add or update mobile agent-based applications to work concurrently and independently from each other. Security mechanism is employed at middleware layer. This solution is feasible and effective for WSNs:

- Sink hole attack In Sink Hole attack malicious node acts as a black hole to attract all the traffic in the sensor network. Attacker listens to requests for routes then replies to the target nodes. It inserts itself between the communicating nodes; it can do anything with the packets passing between them.
- Cloning attack, A node replication attack involves an attacker inserting a new node into a network which has been cloned from an existing node, such cloning being a relatively simple task with current sensor node hardware. This new node can act exactly like the old node, or it can have some extra behavior.
- Mobile agent Mobile Agent is defined as a software component which is used to perform the network function or application Mobile agents can be aware of network failures. Therefore, mobile agents allow a great degree of flexibility regarding which data is collected. [7]

C. Mobile Appliances

The evolution of the Internet, information and communications security has already gained significant attention. Whereas the knowledge and experience gained from the wired Internet, including cryptographic algorithms, security protocols, and standards, give us a head start in the quest to secure mobile appliances, there are several challenges unique to mobile appliances that must still be addressed.

Mobile appliances often use a public transmission medium for communication, which implies that the physical signal is easily accessible to eavesdroppers and hackers. Wireless security is a challenging problem, perhaps even more so than wired security in many respects, that must be addressed by many mobile appliances.

Mobile appliances are quite vulnerable to theft, loss, and corruptibility. Security solutions for mobile appliances must, therefore, provide for security under these challenging scenarios. Constraints on cost and weight, and the need to operate mobile appliances off batteries, imply that they are quite constrained in their processing capabilities and energy supplies. The processing and energy overhead required to provide sufficient security can be significant and overwhelm the modest capabilities of mobile appliances. The challenges of securing mobile appliances can be adequately addressed only through measures that span virtually every aspect of their design hardware circuits and micro-architecture, system architecture, system and application software, and design methodologies. This paper introduces the new challenges that security poses to mobile appliance designers, and surveys technologies that can be used to address them. Despite significant recent interest and notable innovations in this area, many challenges remain that will require further attention and awareness of security among hardware, software, and system designers. [5]

D. Principal Component Analysis

We then joined the feature set that was removed before both the filter was applied with the feature set obtained after the application of filters. We applied the dimensionality reduction technique called the

Principal Component Analysis (PCA). This technique helps in reducing the feature space by transforming the features into features with a high variance. The newly produced features or the principal components as we call them, are ranked with the first principal component being the best representation of all the features and so on. We chose first two principal components for our unsupervised learning technique.

E. Data Analysis using K-means Clustering

We applied K-means clustering on obtained principal components. We first normalized our principal components in the range [0,1]. This was done to ensure that there are no negative values, and the cluster shape are not arbitrary. If the range would have been kept from [-1,1], the cluster obtained were in the shape of a circumference of circle. This was because it had some values going into the negative region. We then applied K-means clustering for K=2,3...10 clusters. We used the pre-defined function provided in the python library to perform the clustering. Since, we had no pre-defined labels to compare our results with, therefore, we went with K=2 clusters. The clusters obtained when K=2 is shown in Fig 2. below.

4. CONCLUSION

In this paper we have discussed most of the major security flaws in the WEP protocol and described several practical attacks. Also, we saw that WEP cannot be fully reliable for a strong link-level security, and that additional precautions be taken to protect network traffic.

We also made use of the polynomial bivariate key exchange scheme for wireless sensor network with mobile sink. Those key exchange between the sink and the sensor node of that only the authenticate nodes involve in the communication other nodes are not involved. This makes it difficult for the attackers to get the original information.

Security is an important in that wide range of applications involving mobile appliances. This paper highlights some of the many problems that we come across the mobile appliances. Security concerns are not limited to a specific application domain but cut across a wide range of electronic systems. Hence, we believe that security will increasingly impact various aspects of the system design process, including hardware circuits and microarchitecture, software, system architecture, and design methodologies

REFERENCES

[1] N. Borisov, I. Goldberg, and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11. In Proceedings of the International Conference on Mobile Computing and Networking, 2001.

[2] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker, Security Flaws in 802.11 Data Link Protocols. In CACM May 2003.

[3] Russ Housley and William Arbaugh , Security Problems in 802.11-based Networks . In CACM May 2003.

[4] A. Stubblefield, J. Ioannidis, and A. Rubin, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In Proceedings of the 2002 Network and Distributed Systems Security Symposium, 2002

[5] Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater, Securing Mobile Appliances: New Challenges for the System Designer, Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03, Mar. 2003

[6] Saahira Banu Ahmed; Ananthi Shesasayee, To enhance security in wireless sensor networks with mobile sink, Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014

[7] A. Vijayalakshmi; T. Shrimathy; T. G. Palanivelu, Mobile agent middleware security for Wireless Sensor Networks, 2014 International Conference on Communication and Signal Processing 2014

[8] Amar Rasheed; Rabi N. Mahapatra, The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks, IEEE Transactions on Parallel and Distributed