AUTHENTICATION PROVISION FOR WSN BASED ON MULTI LEVEL SECURITY

R. Vissu Pon Thangam*

S. Muthu Kumar*

Abstract—

Mobile Sinks (MSs) are very important in many wireless sensor networks (WSN) applications for efficient accumulation of data, sensor reprogramming that is localized, and for distinguishing and revoking compromised sensors. This paper describes a three-tier general framework that permits to provide a platform for various applications that can improve safety and efficient group communication. One of them is multicasting networks. In existing system, Tiered Authentication scheme for Multicasting (TAM) is used for the multicast traffic in ad-hoc networks. Two tiered hierarchy combines the time and secret-information asymmetry to achieve the resource efficiency and scalability. In proposed system, an Asynchronous authentication scheme using shared key management is to resolve the most conflicting security requirements such as group authentication and conditional privacy.

Keywords—Distributed networks, Network security, wireless sensor networks.

* PSN College of Engineering and Technology, Tirunelveli.

I. INTRODUCTION

THE wireless and mobile networks represent an increasingly important segment of networking research as a whole, driven by the rapid growth of portable computing, communication and embedded devices connected to the Internet. The advances in electronic technology have paved the way for the development of a new generation of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly. mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) 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. 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. Developing 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, first cultivated a general three-tier security framework for authentication and pairwise key establishment. Overall, it is clear that mobile, wireless and sensor devices will certainly outnumber wired end-user terminals on the Internet in the near future, strongly motivating consideration of fundamentally new network architectures and services to meet changing needs.

Over the next 10-15 years, it is anticipated that significant qualitative changes to the Internet will be driven by the rapid proliferation of mobile and wireless devices, which may be expected to outnumber wired PC’s as early as 2010. The potential impact of the future wireless Internet is very significant because the network combines the power of computation, search engines and databases in the background with the immediacy of information from mobile users and sensors in the foreground. Wireless networks are of a fundamentally different character: To begin with, wireless connections are by nature significantly less stable than wired connections. Effects influencing the propagation of radio signals, such as shielding, reflection, scattering, and interference, inevitably require routing systems in ad hoc networks to be able to cope with comparatively low link communication reliability. Also, many scenarios for ad hoc networks assume that nodes are potentially mobile.

Another critical issue during natural or man-made disasters is that the situations changes rapidly, in most of the cases in unpredictable ways, and it is almost impossible, using the normal channels of communication, to avert and direct the population. For example people trying to escape from flooding caused by hurricanes, may choose damaged roads, bridges, or tunnels that could become mortal traps. Another scenario is that of a terrorist attack in a subway or a building. People trying to escape via a more obvious way, may go toward closed exits, even more dangerous locations such as fire and poison.

The revolutionary advances in the wireless communication technologies are enabling the realization of a wide range of heterogeneous wireless systems. This technological development is further inspiring the researchers to envision several scenarios: Constellation of Wireless Devices (Mobile Ad hoc Networks), Pervasive Systems and Sensor Networks, and Emergency Ad hoc Cellular Networks.

1. *Constellation of Wireless Devices*

A Mobile Ad hoc Network consists of wireless Mobile Nodes (MNs) that cooperatively communicate with each other without the existence of fixed network infrastructure. Depending on different geographical topologies, the MNs are dynamically located and continuously changing their positions. The fast-changing characteristics in ad hoc networks make it difficult to discover routes between MNs. It becomes important to design efficient and reliable multi-hop routing protocols to discover, organize, and maintain the routes in ad hoc networks. An area where there is much potential for wireless technologies to make a tremendous impact is the area of vehicular ad hoc networks (VANET). There are numerous emerging applications that are unique to the vehicular setting. For example, safety applications would make driving safer; driver information services could intelligently inform drivers about congestion, businesses and services in the vicinity of the vehicle, and other news. Mobile commerce could extend to the realm of vehicles. Existing forms of entertainment may penetrate the vehicular domain, and new forms of entertainment may emerge

2. *Pervasive Systems and Sensor Networks*

Recent advances in wireless communications and micro electro-mechanical systems have enabled the development of extremely small, low-cost sensors that possess sensing, signal processing, and wireless communication capabilities. These sensors can be deployed at a much lower cost than that of traditional wired sensor systems. An ad hoc wireless network of large numbers of such inexpensive but less reliable and accurate sensors can be used in a wide variety of commercial and military applications such as target tracking, security, environment monitoring, and system control. Wireless sensor networks are expected to be the basic building block of pervasive computing environments. Aggregating sensor nodes into sophisticated sensing, computational and communication infrastructures to form wireless sensor networks will have a significant impact on a wide array of applications ranging from military, to scientific, to industrial, to health-care, to domestic, establishing ubiquitous computing that will pervade society redefining the way in which we live and work.

3. Emergency Ad hoc Cellular Networks

A cell phone is essentially a battery-powered microprocessor with one or more wireless transmitters and receivers optimized for voice I/O. Even a bare-bones model provides a keyboard, an LCD screen, and a general-purpose computing platform, typically supporting Java2 Mobile Edition (J2ME) or .NET Compact APIs. More sophisticated models provide a camera, 1MB-5GB of local storage, a full-color screen, multiple wireless interfaces, and even a QWERTY keypad. Today's cellular networks use fixed infrastructures, which are vulnerable to the disaster effects like hurricanes and terrorist attacks. One scenario is that cellular phones switch to an ad hoc mode when their fixed infrastructure is no longer functioning. The advantage of using cellular phones in disaster/emergency conditions is that everyone has one; therefore, the communication tools will be always ready, even when the unexpected happens. It is very important to consider conditions and restrictions created by emergency and disaster situations.

For example, in disaster conditions, which duration is unpredictable, saving energy becomes an important goal, as it may be impossible to charge cellular phones. Another critical issue during natural or manmade disasters is that the situations changes rapidly, in most of the cases in unpredictable ways, and it is almost impossible, using the normal channels of communication, to avert and direct the population. For example people trying to escape from flooding caused by hurricanes, may choose damaged roads, bridges, or tunnels that could become mortal traps. Another scenario is that of a terrorist attack in a subway or a building. People trying to escape via a more obvious way, may go toward closed exits, even more dangerous locations such as fire and poison. Terrorists may plan their attacks by taking into account the victims' most likely reaction. Therefore, we need protocols that enable quick and efficient delivery of information to people. The source of information could be other users, officials, or generated by sensing devices. Finally, we need ways to guarantee communication and interoperability between the area under disaster and the unaffected areas.

II. Related Work

Wireless communication is much more difficult to achieve than wired communication because the surrounding environment interacts with the signal, blocking signal paths and introducing noise and echoes. As a result wireless connections have a lower quality than wired connections: lower bandwidth, less connection stability, higher error rates, and, moreover, with a highly varying quality. These factors can in turn increase communication latency due to retransmissions, can give largely varying throughput, and incur high energy consumption. In this section, we discuss a set of protocol design issues related to the networking requirements of the representative wireless scenarios identified earlier.

• *Quality of Service*

Since wireless networks deal with the real world processes, it is often necessary for communication to meet real-time constraints. In battle surveillance systems, for example, communication delays within sensing and actuating loops directly affect the quality of enemy tracking. Due to the nature of the wireless communication and unpredictable traffic pattern, it is infeasible to guarantee hard real-time constraints; however, research that provides probabilistic guarantee for timing constraints is quite achievable and essential.

• *Heterogeneity*

In contrast to most stationary computers, mobile device encounter more heterogeneous network connections. As they leave the range of one network transceiver they switch to another. In different places they may experience different network qualities. There may be places where they can access multiple transceivers, or even may concurrently use wired access. The interface may also need to change access protocols for different networks, for example when switching from wireless LAN coverage in an office to cellular coverage in a city. This heterogeneity makes mobile computing more complex than traditional networking.

• *Large Scale*

Smart hospitals, battlefields and earthquake response systems are applicable sensor network systems. Such systems require a large geographic coverage. At the same time, a high density is required to work against the high failure rate of sensor nodes, the low confidence in individual sensor readings, the limited communication range and low capability of single sensor nodes. Due to these reasons, sensor networks are expected to scale up to thousands and millions of nodes, two orders of magnitude larger than traditional ad hoc networks.

• *High Unpredictability*

Sensor network applications are driven by environmental events, such as the earthquake and fire, anywhere anytime following an unpredictable pattern. Sensor node failures are common due to the sheer number of sensor nodes and the hostile environment. The radio media shared by densely deployed nodes is subject to heavy congestion and jamming. High bit error ratio, low bandwidth and asymmetric channel make the communication highly unpredictable. Such unpredictability usually prevents off-line design of system parameters. Online monitoring and feedback control are required to provide a certain degree of QoS guarantee under such situations.

• *Robust Data Delivery under Failure and Mobility*

Sensor networks are faulty networks where failures should be treated as normal phenomena. Unreliable nodes, constrained energy, high channel bit error ratio, interference and jamming, multi-path-fading, asymmetric channel and weak security make the communication highly unreliable. At same time, sensor networks are highly dynamic networks where network topologies are constantly changing due to a high rate of node failure, changes of power modes, and nodes' mobility.

• *Energy-efficiency*

The wireless network interface of a mobile computer consumes a significant fraction of the total energy of a mobile computer. More extensive and continuous use of network services will aggravate this problem. Energy efficiency can be improved at various layers of the communication protocol stack.

• *Adaptive*

Wireless networks is challenging because of the unpredictable behavior of the medium and the proactive effect of interference. Compared to the wired networks the degree of variability of the state of wireless networks is quite high. Also the performance of the network, in terms of delay and throughput, is highly dependent upon the state of the network. The effects of the state of a wireless network are spread across several layers. Thus in order to meet the requirements of the application despite variable link state, network topology and power levels, it is important that the layers coordinate and adapt to the change in network state.

To deal with the dynamic variations in networking and computing resources gracefully, both the mobile computing environment and the applications also need to adapt their behavior depending on the available resources including the batteries.

III. Three Tier Security Scheme

Recent advances in electronic technology have paved the way for the development of a new generation of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. Mobile sinks are the receiving stations of the message transmission. This mobile sinks are receiving the messages through the access points of the message transmission process. Sensors are the sender of the messages to the mobile sinks through the access points.

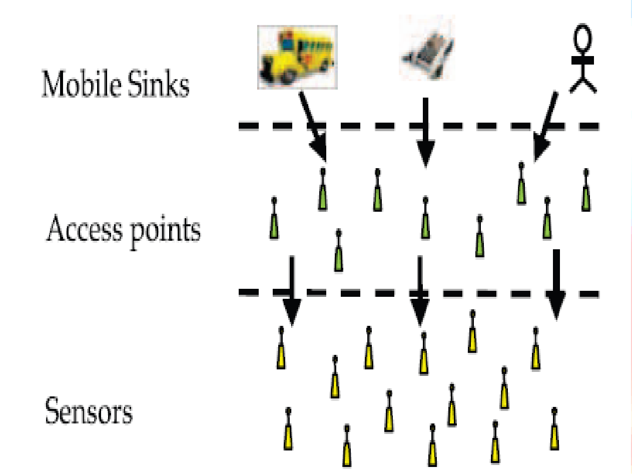

Fig.1 Three-tier security scheme in WSN with mobile sinks

This three-tier security schemes are used for the communication between many senders and receivers. This communication process is essential for group communication. It protects the messages through the encryption and decryption techniques and provides the multi-level security for the group communication. The key management problem is an active research area in wireless sensor networks.

Sources of Challenges in Wireless Networks

There are many features of the wireless medium that distinguish it from other media. The wireless medium is a shared medium. This means that unlike wire line systems, where there exist dedicated physical connections between users, every user can essentially receive an attenuated version what other users are transmitting. In such a system, the manner of transmission is broadcast of the signal and there is interference in reception of a signal. Another property of a wireless channel is its random time- varying behavior due to the mobility of users and other objects, as well as obstacles in the environment.

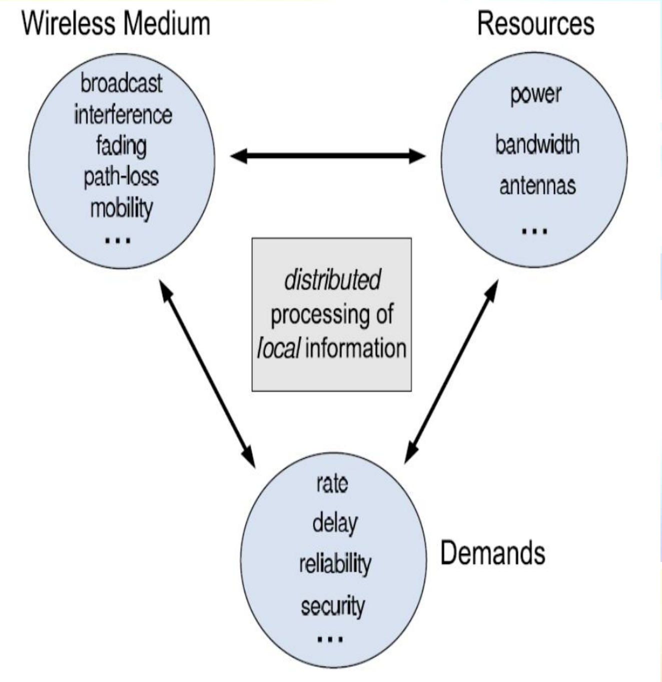

Fig.2 Sources of challenges in analysis and design of wireless networks

More specifically, the channel to a given user might have poor conditions at some times and favorable conditions at other times. This is called the fading behavior of the channel. In many situations, multiple copies of the transmitted signal may be received with different delays and different strengths. This is referred to as “multipath fading" and can severely deteriorate the performance when the transmitted signals have shorter duration (e.g., broadband transmission). Conventionally, the goal is to combat the randomness introduced by the environment. However, in recent years, there has been another view and that is to exploit the inherent randomness in the environment to increase the performance.

For instance, the multi-user diversity gain in the downlink of cellular systems is based on this idea, i.e., in a system of many users with random quality of reception (fading), there exists one user with good quality of reception with very high probability.

Efficient Use of Resources

Today's wireless systems are faced with an ever-growing demand for higher rates and quality of services. However, the available resources such as bandwidth, power, and number of antennas are limited. Therefore, efficient usage and allocation of these resources is more important than ever. In many scenarios, from mobile users in cellular networks to sensor nodes deployed in a remote area, the components of the network have limited power supplies. In these networks, efficient use of the available energy (power) supply is a critical issue. Bandwidth is another valuable resource in wireless systems, especially in high data rate broadband communications. Also, there has been a great interest in exploiting the spatial degrees of freedom in wireless systems by deploying multiple antennas at the transmitter and the receiver. The possibility of using multiple antennas in a network (multi-user) setup has been recently explored.

Demands and Services

As mentioned earlier, wireless systems have become highly heterogeneous. Different types of applications such as voice, internet, and video-on-demand, are provided over wireless networks. Depending on the application, the main performance measure will vary. For instance, video-on-demand applications not only require high rates but also are sensitive to delay. For many detection schemes, in ad-hoc networks reliability is the main concern. In many scenarios, resource allocation in wireless networks aims at optimizing over two conflicting performance measures at the same time, such as reliability and rate or delay and rate. Finding strategies that provide these different demands in an efficient manner is a challenging task.

IV. Modules Description

The topology formed the network and then transmitted the information for managing the key values. The key management process managing the key by the intra and inter clustering techniques. Then only the key establishment process occurred by the hash functions of the key values. Using the hash function, the process of transmitting the information with the secret key is very easy. The analysis process is calculating the time delay and the bandwidth overhead.

a. Architectural Model

The simulation work has been done with The Network Simulator ns-2, Version 2.29. In the simulation 50 nodes are randomly distributed within the network field of size 2400mx2400m. Ad hoc network topology is formed with the help of various nodes creation. Clusters are formed based on the location and their connectivity with other nodes.

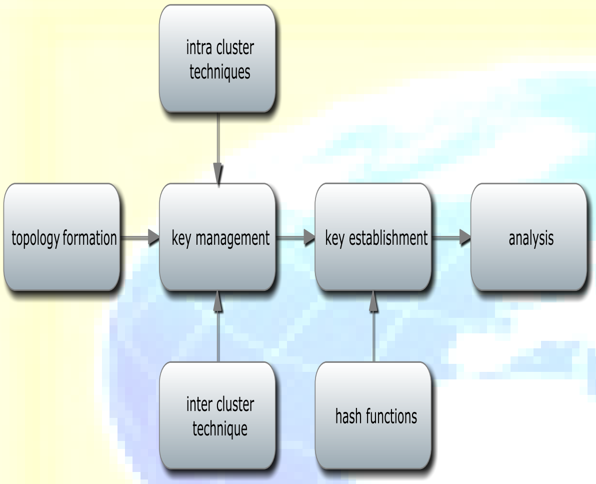

Fig.3 Architectural Model

Each cluster is controlled by the cluster heads from them only messages are passed to another cluster. Source nodes are in connection with cluster heads.

b. Key Establishment

In this paper use RSA based key generation. And then use of hashing technique for memory optimization. Then create one pair wise key and one shared key. After the creation of these keys, the authentication process will start for the intra and inter communication through the wireless sensor networks. Network Animator is presented information such as throughput, number packets on each link.

c. Group Key Management (Intra Cluster)

Nodes get keys dynamically in the key distribution phase and then start to broadcast their geographic based. All nodes getting keys from the same leader form a group, as illustrated in the communication range of RSUs is 300 meter. The key was asymmetric based group key method in both Leader and member have a common key for sharing. This group key identifies the cluster head and provides the authentication between the clusters. The cluster head helps to provide the secured information to its cluster. The information can transmit within the cluster.

d. Shared Key Management (Inter Cluster)

Leaders get keys dynamically in the key distribution phase and then start to broadcast their geographic condition messages. All leader nodes getting keys from the server form, as illustrated in the communication range of leader is 300 meter. If one cluster head has the key, it will provide the key for authentication for each cluster head. Then the leader shares the key between all cluster heads. The key was asymmetric based shared key method in each cluster heads have a common key for sharing.

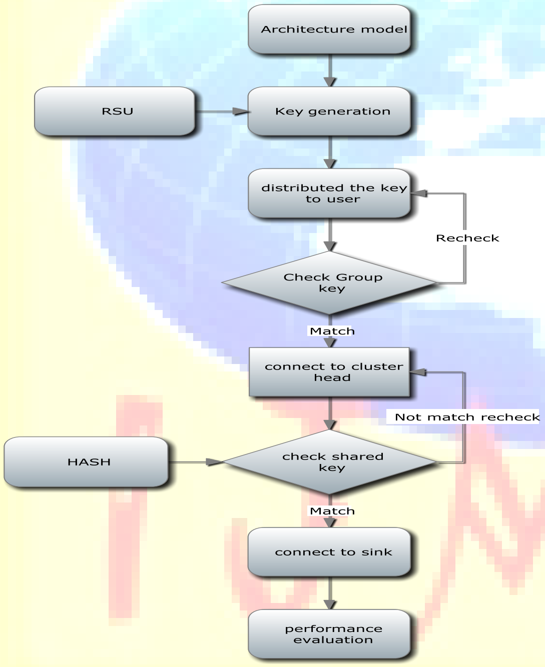

Fig.4 flow diagram

e. Performance Evaluation

Compare both the theoretical and simulation results under our protocol with those under the protocol in. Since the cooperative authentication protocol is of particularly importance in the high-load scenario, thus only focus on the highway scenario in this part. Assume six percent of the vehicles are malicious in our simulations. Malicious vehicles always send invalid RBM.

V. Operation Techniques

Operation in a Network Setup

Finding the optimal strategy for the nodes of a network in order to optimally perform a given task is very much an open problem. Consider the simple network, with only three nodes, in the above figure. The desired task is reliable communication from the source to the destination with the aid of the relay node. The relay node is connected to both the source and destination through communications channels. Even for this simple network, finding the optimal operation at each node for maximizing the rate of reliable communication is unsolved. The main difficulty in a network setup is the distributed nature of the information in the network. Each user has only access to local information and has to cooperate with other nodes in a distributed fashion to maximize the performance.

The above sources have raised many important and interesting challenges regarding the performance limits of different tasks such as communications and computation over networks.

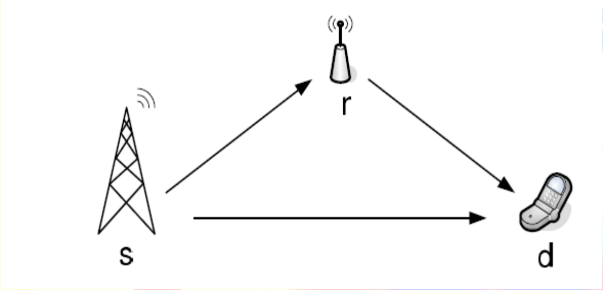

Fig.5 A simple network with one relay component, one source and one destination

In addition, there are many design issues concerning the complexity and the robustness of the systems that should be addressed for a thorough understanding and efficient operation of wireless networked systems.

Security and Multicasting: a Complex Deal

The IP multicast model is attractive because it can scale to a large number of members. However, scalability is achieved due to the fact that no host identification information is maintained by the routers. Any host in a subnet can join a multicast group without its subnet router passing identification information about the host to other routers in the distribution tree. This simplicity which makes the strength of multicast routing, presents however, many vulnerabilities:

1. IP multicast does not support closed groups In fact, multicast addresses are publicly known: joining or leaving a group does not require specific permissions. Hence, any user can join a multicast group and receive messages sent to the group.

2. There is no access control to a multicast group: An intruder can send data to the group without being a valid member, and disturbs the multicast session or eventually create bottlenecks in the network (Denial of Service attack).

3. Data sent to the group: It may transit via many unsecure channels. Thus, eavesdropping opportunities are more important.

VI. Security Threats And Countermeasures

There exist many security threats, inherent to the distributed and open nature of IP multicast, that require security countermeasures.

1.*Denial of Service / Access Control:*

In the basic IP multicast model, any node can send data to a multicast session, and any node can become a member of any multicast session. It is clear that this model is vulnerable to Denial of Service (DoS) attacks, where fraudulent users join or send data to multicast sessions only to waste bandwidth or to overwhelm other group members with garbage data or malicious code. Solving these problems requires controlling the ability of hosts to send data or to join a multicast tree distribution. These are called respectively: sender and receiver access control.

2.*Eavesdropping / Confidentiality:*

In unicast communication, two users can provide confidentiality by encrypting data with a shared key. In multicast communication, a group key is given to every authorized member. This group key is used by the sender as a symmetric key to encrypt the multicast traffic. This becomes complicated when group membership is dynamic (members join and leave continuously the multicast session). Research work in group key management aims to provide efficient re-keying schemes for dynamic membership groups.

3. *Masquerading / Data Origin Authentication:*

Data origin authentication is the ability of group members to verify the identity of the sender of a received packet. There has been work that aims to efficiently provide this level of authentication.

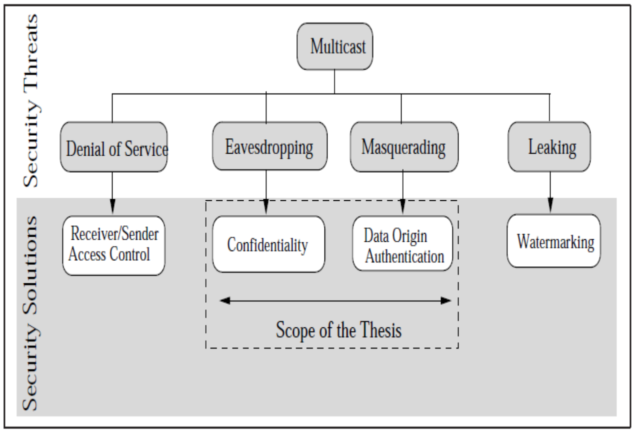

Fig.6 Multicast Security Threats and their Countermeasures

4.*Leaking / Water marking:*

Encryption is generally used to safeguard content while it is being transmitted so that unauthorized persons cannot read the stream from the network, but this offers no protection after the intended receiver receives the data. There is no protection against unauthorized duplication and propagation by the intended receiver. Watermarking can provide protection in the form of theft deterrence. Watermarking is the embedding of some identifying information into the content in such a way that it cannot be removed by the user but can be extracted or read by the appropriate party.

VII. Conclusion

Here TAM Tiered Authentication scheme for multicast session. It is used to authenticate the source and to prevent the messages from the intruders. To authenticate the message source one-way hash chains is used within the same cluster. The authentication code is appended to the message body. The authentication key is exposed after the message is delivered. Two tired security scheme for time and secret information asymmetry in order to achieve the scalability and resource efficiency and to extend the implementation with RSA 3 key generation techniques. With a public key (PKA) or asymmetric key algorithm, a pair of keys is used to achieve the scalability and resource efficiency. RSA encryption, supplies unique and stability technology advantages, presents an authentication system. The one-way hash chains algorithm in conjunction with RSA three key techniques.

References

[1] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,” Proc. MobiCom, pp. 56-67, 2000.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[3] H. Deng, W. Li, and D.P. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” Proc. IEEE Comm. Magazine, pp. 70-75, 2002.

[4] L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002.

[5] H. Chan, A. Perrig, and D. Song, “Random Key Pre-Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.

[6] D. Liu, P. Ning, and R.Li. Establishing, “Pairwise Keys in Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.

[7] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Static Sensor Networks,” Proc. First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.

[8] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 62-72, Oct. 2003.

[9] W. Zhang, G. Cao, and T. La Porta, “Data Dissemination with Ring-Based Index for Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.

[10] L. Hu and D. Evans, “Using Directional Antenna to Prevent Wormhole Attacks,” Proc. Network and Distributed System Security Symp., 2004.

[11] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin, “Intelligent Fluid Infrastructure for Embedded Networks,” Proc. Second ACM Int’l Conf. Mobile Systems, Applications, and Services (MobiSys ’04), June 2004.

[12] B.J. Culpepper and H.C. Tseng, “Sinkhole Intrusion Indicators in DSR MANETs,” Proc. First Int’l Conf. Broadband Networks (Broad-Nets ’04), pp. 681-688, Oct. 2004.

[13] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, “Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors,” Proc.13th Int’l Conf. Computer Comm. and Networks (ICCCN ’04), Oct. 2004.

[14] H. Chan, A. Perrig, and D. Song, “Key Distribution Techniques for Sensor Networks,” Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[15] A. Rasheed and R. Mahapatra, “An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks,” Proc. Third Int’l Conf. Intelligent Sensors, Sensor Networks and Information Processing, 2007.