Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Critical Services for Wireless Sensor Network: Review

Nikhil Sawalakhe*, Seema Ladhe
Department of Computer Engineering
MGMCET, Mumbai University, India

Abstract— Today wireless sensor networks (WSN) is a most challenging technology. In a wireless sensor network (WSNs) broadcast authentication is a critical security service. Wireless sensor network are widely used in environmental control. Authentication is more difficult in Wireless sensor networks. It suffers from several drawbacks like; it takes more time for authentication. In wireless sensor network main problem is maximum buffering, delay, attack and overheads. These all problems are solving by using various protocols and methods. Much research has focused on how to secure wireless sensor networks. In this paper we can discuss various author works, advantages and disadvantages that help to solve all problems. Our contribution is to compare different method for better communication.

Keywords: -- Wireless Sensor Networks, Chinese Remainder Theorem, TESLA, μTESLA, Broadcast authentication.

I. INTRODUCTION

Broadcast authentication is an important security service in wireless sensor network. Example of broadcast distribution networks are satellite broadcast, wireless radio broadcast. In wireless sensor network there is many small sensor node and large number of base stations .Sensor network provide various things like, traffic flows, tracking and maintaining communication flow. The sensors in a node provides the facility to get the data like pressure, temperature, light ,motion, sound etc and capable of doing data processing. The main goal of the applications is achieved by the cooperation of all sensor nodes in the network. There are many sensor networks applications like such environmental data collection, security monitoring, medical science, military, tracking etc. when sensor networks are randomly deployed in a hostile environment, security becomes extremely important factor. Because sensed data of sensor nodes is prone to different types of malicious before reaching base station. Security mechanisms are needed in communication part of the networks to provide safe data. The security is also important concern to get full advantage of network data processing sensor networks. Protecting such a sensed data is complicated task.

A sensor network typically consists of hundreds, or even thousands, of small, low-cost nodes distributed over a wide area. The nodes are expected to function in an unsupervised fashion even if new nodes are added, or old nodes disappear (e.g., due to power loss or accidental damage). While some networks include a central location for data collection, many operate in an entirely Distributed manner, allowing the operators to retrieve aggregated data from any of the nodes in the network. Furthermore, data collection may only occur at irregular intervals. Even through wireless sensor network is an advanced technology of network, it is extremely different from traditional wireless networks. This is, due to the unique characteristics of sensor nodes in WSN. So existing security mechanisms of traditional wireless networks are not directly applied in WSN. Sensor networks are closely interacting physical environment. So sensor nodes are also deployed in all areas even physical accessible attacks and broadcasting sensed data in network. So these reasons give a scope to new security mechanism rather than applying existing traditional security mechanisms in WSN.

II. SECURITY ISSUES

A. *Data Confidentiality:*

A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Given the observed communication patterns, we set up secure channels between nodes and base stations and later bootstrap other secure channels as necessary.

B. *Data Authentication:*

Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver shares a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender.

This style of authentication cannot be applied to a broadcast setting, without placing much stronger trust assumptions on the network nodes. If one sender wants to send authentic data to mutually untrusted receivers, using a symmetric MAC is insecure: Any one of the receivers knows the MAC key, and hence could impersonate the sender and forge messages to other receivers. Hence, we need an asymmetric mechanism to achieve authenticated broadcast. One Of our contributions is to construct authenticated broadcast from symmetric primitives only, and introduce asymmetry with delayed key disclosure and one-way function key chains.

C. *Data Integrity:*

In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. In SPINS, we achieve data integrity through data authentication, which is stronger property.

D. *Data Freshness:*

Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages.

We identify two types of freshness: weak freshness, which provides partial message ordering, But carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.

III. SECURITY CHALLENGE OF WSN

The objective of confidentiality is required in sensors environment to protect information traveling among the sensor nodes of the network or between the sensors and the base station from disclosure. Authentication in sensor networks is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender or not. This authentication is needed during the clustering of sensor node in WSN. We can trust the data sent by the nodes in that group after clustering. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Secure management is needed at base station, clustered nodes, and protocol layer in WSN. Because security issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management.

IV. VARIOUS ATTACKS ON WSN

The basic categories of attacks against privacy in sensor networks are eavesdropping, disruption and hijacking. The eavesdropping is used to know the output of sensor networks by listing transmitted messages of sensor nodes. There are mainly two ways to know about output data by concealing from sensor nodes or sending queries to sensor nodes or root nodes or aggregation points or attacks sensor nodes. The former approach is called passive eavesdropper and later approach is called active eavesdropper. The location of eavesdropper plays major role in getting information. This attack affects the property of confidentially, authentication in WSN. So proper encryption mechanism, message authentication code are needed before broadcasting data. The disruption mainly influences output of the network. The semantic disruption injects messages, corrupts data or changes values in order to render the aggregate data corrupted, useless and incomplete.

Physical disruption renders the sensor readings by directly manipulating the Environment. The hijacking approach is used to take the control over sensor node in network. The hijacking mechanism gives more power to eavesdropping and disruption by hijacking main Sensor nodes. Another major attack in WSN is Denial of Service attacks. Some of the denial of service attack are at routing layer, link layer and transport layer. One of the denials of service attack is jamming networks. That is simply interfaces transmission frequency of WSN.

There are mainly two types in jamming. In constant jamming, no messages are able to send or receive by a node in WSN. So this is complete jamming of network. In Intermittent jamming, the nodes are exchange messages with highly risks. Another new attack in WSN is Sybil attack. This Sybil attack is defined as a "malicious device illegitimately taking on multiple identities".This attack is affecting redundancy mechanism, routing algorithms, resource allocation procedure and data aggregation mechanism. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. They may allow the adversary to corrupt network data or even disconnect significant parts of the network. This attack can change entire network goal. This attack affects Integrity, confidentiality.

A. *Denial of Service (DoS) Attack:*

Denial of service (DoS) attacks has become a major threat to current computer networks. Early DoS attacks were technical games played among underground attackers. For example, an Attacker might want to get control of an IRC channel via performing DoS attacks against the channel owner. Attackers could get recognition in the underground community via taking down popular web sites. Companies might use DoS attacks to knock off their competitors in the market. Extortion via DoS attacks were on rise in the past years. Attackers threatened online businesses with DoS attacks and requested payments for protection. Known DoS attacks in the Internet generally conquer the target by exhausting its resources that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. Because it is difficult for attackers to overload the target's resource from a single computer, many recent DoS attacks were launched via a large number of distributed attacking hosts in the Internet. These attacks are called distributed denial of service (DDoS) attacks. In a DDoS attack, because the aggregation of the attacking traffic can be tremendous compared to the victim's resource, the attack can force the victim to significantly downgrade its service performance or even stop delivering any service. Compared with conventional DoS attacks that could be addressed by better securing service systems or prohibiting unauthorized remote or local access, DDoS attacks are more complex and harder to prevent. Since many unwitting hosts are involved in DDoS attacks, it is challenging to distinguish the attacking hosts and take reaction against them. In recent years, DDoS attacks have increased in frequency, sophistication and severity due to the fact that computer vulnerabilities are increasing fast which enable attackers to break into and install various attacking tools in many computers. Wireless networks also suffer from DoS attacks because mobile nodes (such as laptops, cell phones, etc.) share the same physical media for transmitting and receiving signals; and mobile computing resources (such as bandwidth, CPU and power) are usually more constrained than those available to wired nodes. In a wireless network, a single attacker can easily forge, modify or inject packets to disrupt connections between legitimate mobile nodes and cause DoS effects.

B. *Node Replication:*

Security is one of the top design criteria for many sensor networks, particularly for large-scale military deployment involving thousands of sensor nodes that perform critical tasks in hostile areas. These areas are sometimes physically accessible to camouflaged enemies. If an adversary manages to capture a sensor and extract the authentication/encryption keys, it can produce a large number of replicas with the keys and integrate them into the sensor network at chosen locations, which is called the node replication attack.

C. *Physical Attack:*

Physical attacks are inevitable threats in sensor networks due to the small form factor of sensors, and the unattended and distributed nature of their deployment. Physical attacks are relatively simple to launch and destructive. In the simplest case, the attacker can just drive a vehicle in the sensor eld or hurl grenades/bombs in the eld and destroy the sensors. A smarter attacker can detect and destroy sensors with stealth by moving across the sensor network. In any case, the end result of physical attacks can be quite destructive. The backbone of the network (the sensors themselves) is destroyed. Destruction of sensors may also result in the violation of the network properties (topology, routing structure etc). As such, a wide spectrum of impacts may result due to physical attacks, and when left unaddressed, physical attacks can destroy the entire sensor network mission.

D. *Modification:*

Unauthorized party not only accesses the data but also tampers with it. This threatens message integrity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer, because of the richer semantics of these layers.

E. *Outsider versus insider (node compromise) attacks:*

Outside attacks are defined as attacks from nodes, which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. To overcome these attacks, we require robustness against Outsider Attacks, Resilience to Insider Attacks, Graceful Degradation with Respect to Node Compromise and Realistic Levels of Security.

F. *Attacks on Information:*

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be attacked to provide wrong information to the base stations.

V. PROTOCOLS USED IN WSN

A. *Access Control Medium Protocols:*

Medium Access Control (MAC) protocols that have been designed for typical ad hoc networks have primarily focused on optimizing fairness and throughput efficiency, with less emphasis on Energy protection. However, the energy limitation is typically considered paramount for wireless sensor networks, and so many MAC protocols have recently been designed that tailor themselves specifically to the characteristics of sensor networks. However, it has been shown that idle power consumption can be of the same order as the transmit and receive power consumption, and if so, can greatly affect overall power consumption, especially in networks with relatively low traffic rates. Thus, the focus of most MAC protocols for sensor networks is to reduce this idle power consumption by setting the sensor radios into a sleep state as often as possible.

B. *Data-Centric Routing Protocols*:

Sensor networks are fundamentally different from ad hoc networks in the data they carry. While in ad hoc networks individual data items are important, in sensor networks it is the aggregate data or the information carried in the data rather than the actual data itself that is important. This has led to a new paradigm for networking these types of devices – data-centric routing. In Data-centric routing, the end nodes, the sensors themselves, are less important than the data itself. Thus, queries are posed for specific data rather than for data from a particular sensor and routing is performed using knowledge that it is the aggregate data rather than any individual data item is important.

C. Sensor Protocol for Information via Negotiation (SPIN):

SPIN is a protocol that was designed to enable data-centric information dissemination in sensor networks. Rather than blindly broadcasting sensor data throughout the network, nodes receiving or generating data first advertise this data through short ADV messages. The ADV messages Simply consist of an application-specific meta-data description of the data itself.

D. *Proactive Protocol:*

Proactive routing protocol works completely different than reactive routing protocols. These protocols continuously maintain the information of updated topology of the network. Every node in the network knows in the advance about the other nodes in the network. That is each node knows about complete network. In reactive protocol each node knows about next hop but in proactive protocol each node have complete information of network. All the routing information kept in tables. Whenever there is change in topology, these tables get updated according to change in topology. This node transfers the information with each other. Therefore they have routing information when they needed and any time.

E. *Ad-Hoc On Demand Distance Vector Protocol (AODV):*

AODV is most commonly used reactive protocol in MANET, when any node wants to start communication with another node in the network for which it has no active route. AODV will give information regarding topology to node. AODV uses three control messages to find active path with minimum hop count and to gather topology information. Following are the messages used in AODV.

F. *Route Request Message (RREQ):*

Source node that wants to communicate with another node wishes to find out path to reach initiate route request message and floods that message through the network. The message uses expanding ring technique while travelling across network. An additional information carries with this message is Time to Live (TTL) so that message can reach up to maximum hop count only.

G. *Route Reply Message (RREP):*

A node that's address gets matched with destination address in RREQ sends route reply message to originator. Intermediate node might have active route to that destination also create RREP message and send.

H. *Route Error Message (RERR):*

Every node in the network monitors neighbor's link status. If any node finds any link break or link down so, it is im possible to reach to next node then it generate route error message and inform to other node that link is down.

VI. METHOD USED IN WSN FOR AUTHENTICATION

A. Chinese *remainder theorem:*

Chinese Remainder Theorem (CRT) provides unique solution to receiver side. Receiver receives that solution and compare with MAC address. At the same time base station broadcast the message and CRT solution. After receiving CRT solution receiver recover the MAC of message and authentication key. Receiver uses a one way hash chain to verify the authentication key. After this process it broadcast the message instantly.This scheme has following three phases:

1. *Pre-distribution phase:*

Step 1: Base station forms one way chain for self authentication. After that it selects random value. For example kn is last key in the keys.

Step 2: Then applying one way hash function to derive all earlier keys. Base station generates two keys for broadcasting. And these keys are comparative prime.

Step 3: finally base stations store keys in each sensor memory.

2. Message signing:

Step 1: Base station first sign the message for calculating congruent equation. Base station calculates MAC of the message to solve the equation.

Step 2: check the equation it is congruent or not. If the equation is congruent then it go to the next step otherwise it rollback to first step and sign message again.

Step 3: After getting proper congruent equation, base station broadcast the message immediately.

3. Message Authentications:

Step1: For verification of packets sensor nodes have received the broadcast packets. Sensor nodes check the message and verify using unique solution.

Step2: After checking if it is correct then authenticate it otherwise received message has modified.

Step 3: If message is not correct then it is tampered and sensor node reject that message. Suppose message is correct then it is not tampered.

A. µTESLA:

µTESLA is a lightweight protocol and use for broadcast the message. µTESLA unicasts it by using the secret key shared between the sender and receiver. It is an extension of the TESLA protocol tailored for sensor networks to reduce the computation overhead. JUTESLA is a symmetric-key based broadcast authentication algorithm that periodically broadcasts key authentication packets in sensor networks. A one-way key chain is used for generating the Symmetric keys for message authentication; the asymmetry property required for authentication is introduced by having the sender use a key disclosure delay interval to delay revealing the key to receivers. ,uTESLA uses unicasting to distribute the initial information to each receiver, it may have a large communication overhead in a large-scale sensor network.

B. *TESLA:*

TESLA authenticates the initial packet with a digital signature. Clearly, digital signatures are too expensive to compute on our sensor nodes, since even fitting the code into the memory is a Major challenge. For the same reason as we mention above, onetime signatures are a challenge to use on our nodes. Standard TESLA has an overhead of approximately 24 bytes per packet. For networks connecting workstations this is usually not significant. Sensor nodes, however, send very small messages that are around 30 bytes long. It is simply impractical to disclose the TESLA key for the previous intervals with every packet.

VII. METHODS USED IN WSN FORAUTHENTICATION

A. Chinese Remainder Theorem-Based Broadcast Authentication in Wireless Sensor network: CRTBA [1]

In this paper, we propose a novel protocol, Chinese Remainder Theorem Broadcast Authentication (CRTBA), for wireless sensor networks. CRTBA uses Chinese Remainder Theorem to associate the authenticating procedure of the authentication key and the Message Authentication Code of broadcast messages together. The proposed scheme has the advantage that no time synchronization is required and then the receiver can authentication packets instantly without buffering packets. The analysis shows that this scheme is efficient and practical, and can achieve better performance than the µTESLA. We first use the one-way hash chain of the authentication key of to verify the authentication key and then use the authenticated CRT solution to verify the broadcast message. The analysis shows that our scheme has many Properties, including instant authentication, low overhead in computation, communication and storage.

B. On Optimal Key Disclosure Interval for µTESLA[2]:

Analysis of Authentication Delay versus Network Cost TESLA is an efficient broadcast authentication scheme for sensor networks. In this paper, a simple SPN model to quantitatively analyze µTESLA performance. A goal of this paper is to motivate an analytical approach to studying the optimization of security protocol parameters subject to tradeoffs between application-specified requirements and network cost. In spite of the model's simplicity, some useful insights into the optimization of u TESLA have been obtained.In µTESLA when the time interval T increases, the delay and rejection probability will increase. We analyzed the maximum allowable time interval Top, that will minimize the authentication communication cost while satisfying application-imposed constraints on data authentication delay and data rejection probability. Our analysis results showed that Toptexists and Topt increases as the receiver's buffer size for holding data packets increases; Topt decreases as the key disclosure delay d, the ratio of data broadcast rate to authentication rate, or the key loss probability increases. These results can be used by security systems designers to select the optimal Topt to minimize the network cost in sensor networks, when given a set of parameter values characterizing the application operational environment. Our future work is to incorporate the attacker behavior by malicious nodes and countermeasure designs into our model and Analyze their effects on both security and performance metrics of the resulting system.

C. *Designing secure sensor networks [3]:*

Sensor networks are expected to play an essential role in the upcoming age of pervasive computing. Due to their constraints in computation, memory, and power resources, their susceptibility to physical capture, and use of wireless communications, security is a challenge in these networks. The scale of deployments of wireless sensor networks requires careful decisions and trade-offs among various security measures. The authors discuss these issues and consider mechanisms to achieve secure communication in these networks. Security concerns constitute a potential stumbling block to the impending wide deployment of sensor networks. Current research on sensor networks is mostly built on a trusted environment. Several exciting research challenges remain before we can trust sensor networks to take over important missions.

D. *SPINS: Security Protocols for Sensor Networks [4]:*

We present a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and µTESLA. SNEP provides the following important baseline security primitives: Data confidentiality, two-party data authentication, and data freshness. A particularly hard problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks.µTESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. We implemented the above protocols, and show that they are practical even on minimal hardware: the performance of the protocol suite easily matches the data rate of our network. Additionally, we demonstrate that the suite can be used for building higher level protocols.

We have successfully demonstrated the feasibility of implementing a security subsystem for an extremely limited sensor network platform. We have identified and implemented useful security protocols for sensor networks: authenticated and confidential communication, and authenticated broadcast. To illustrate the utility of our security building blocks, we implemented an authenticated routing scheme and a secure node-to-node key agreement protocol. Many elements of our design are universal and apply easily to other sensor networks. Since our primitives are solely based on fast symmetric cryptography, and use no asymmetric algorithms, our building blocks are applicable to a wide variety of device configurations. The computation costs of symmetric cryptography are low. Even on our limited platform the energy spent for security is Negligible compared with the energy cost of sending or receiving messages. In the absence of other constraints, it should be possible to encrypt and authenticate all sensor readings. The communication costs are also small. Since the data authentication, freshness, and confidentiality properties require transmitting a mere 8 bytes per unit, it is feasible to guarantee these properties on a per packet basis, even with small 30 byte packets. It is difficult to improve on this scheme, as transmitting a MAC is fundamental to guaranteeing data authentication. Certain elements of the design were influenced by the available experimental platform. The choice of RC5 as our cryptographic primitive falls into this category; on a more powerful platform we could use any number of shared key algorithms with equal success. The extreme emphasis on code reuse is another property forced by our platform. A more powerful device would also allow for more basic modes of authentication. The main limitation of our platform was available memory.

E. The TESLA Broadcast Authentication Protocol [5]:

This article presents the TESLA (Timed Efficient Stream Loss-tolerant Authentication) broadcast authentication protocol, an efficient protocol with low communication and computation overhead, which scales to large numbers of receivers, and tolerates packet loss. TESLA is based on loose time synchronization between the sender and the receivers. Despite using purely symmetric cryptographic functions (MAC functions), TESLA achieves asymmetric properties. We discuss a PKI application based purely on TESLA, assuming that all network nodes are loosely time synchronized.

VIII. COMPARISON OF VARIOUS APPROACHES USED TO PREVENT VARIOUS ATTACKS

	CRTBA[1]	Analysis of Authentication Delay versus Network Cost [2]	DESIGNING SECURE SENSOR NETWORKS [3]	SPINS [4]	TheTESLA Broadcast Authentication Protocol [5]
Routing Scheme	CRT	µTESLA	RSA	µTESLA	TESLA
It focuses on	Instant Authentication	Delay verses Network cost	Secure Sensor Network.	Two party data authentication	Authentication
It Reduces	DOS attack	Network cost	Various attack and ambiguous collision	Overheads	Malicious attack
Authentication Scheme	One way hash chain	Symmetric key	Encryption and Decryption	MAC	Message authentication code
Drawbacks	Delay, Overhead are occurs.	Cannot deal with Malicious node	Cannot deal with Outsider attack	High buffering	Untrusted receiver.

IX. CONCLUSION

This paper gives overview of wireless sensor networks, their security issues and generic solutions. Some applications of wireless Sensor network need a secure communication. This paper describes introduction of WSN, Sensor nodes, Methods, protocols types of attack. The existing security models for wireless sensor networks based on specific network models are also reviewed. Approaches for distributed wireless sensor networks must satisfy several security and functional requirements.

REFRENCES

[1] Jianmin Zhang , Wenqi Yu, Xiande Liu, "CRTBA: Chinese Remainder Theorem-Based Broadcast Authentication in Wireless Sensor Networks" , IEEE-2009.

[2] Y.Fan, I.R.Chen and M.Eltoweissy "On Optimal Key Disclosure Interval for µTESLA: Analysis of Authentication Delay versus networkCost," 2005 International Conference on Wireless Networks,Communications and Mobile Computing,vol 13-16 June2005 pp:304- 309

[3] E.Shi,and A.Perrig "Designing Secure Sensor Networks,"IEEE Wireless Communications Vol.11, Dec.2004 pp:38-43.

[4] A. Perrig, R.Szewczyk, V.Wen, D.Culler, and J.Tygar. "Spins: Security protocol for sensor networks," In proceedings of Seventh Annual International Conference On Mobile Computing and Networks, July 2001.

[5] A.Perrig, R.Canetti, J.D.Tygar, and D.Song, "The TESLA Broadcast Authentication Protocol," In CrytoBytes, Summer/Fall 2002, pp:2-13

[6] B.Ramakrishnan,Dr.R.S.Rajesh, R.S.Shaji,"An Intelligent Routing Protocol for Vehicle safety communication in Highway Environments", accepted for publication, journal of computing-dec 2010.

[7] B.Ramakrishnan, R.S.Rajesh, R.S.Shaji," Performance Analysis of 802.11 and 802.11p in Cluster Based Simple Highway Model", IJCSIT, volume 1 issue 5 Nov 2010, page:420-426.

[8] B.Ramakrishnan, R.S.Rajesh, R.S.Shaji," CBVANET: A Cluster Based Vehicular Adhoc Network Model for Simple Highway Communication", Int.J.Advanced Networking and Application Dec-2010, accepted for publication.

[9] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 2010.

[10] D.Liu, P,Ning, S.Zhu, and S.Jajodia "Practical broadcast authentication in sensor networks," Mobile and Ubiquitous Systems: Networking and Services, 2005. July 2005 pp118-129

[11] Y. Hu, A.Perrig, and D. Honson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks." Proceedings of INFOCOM, 2003.

[12] K Ren, W Lou, and Y Zhang, "Multi-user Broadcast Authentication in Wireless Sensor Networks"

[13] K. Ren, K.Zeng, W. Lou and P.J. Moran, "On Broadcast Authentication in Wireless Sensor Networks"