An Efficient Security Framework for Detection and Isolation of Attackers in Low Rate Wireless Personal Area Networks

S.Padma Priya and Mr. Jayaram Pradhan

HOD, Prathyrsha Engineering College, India Bherampur University, Orissa, India

Summary
LR-WPANs pose a number of new security problems in addition to the problems of regular networks. Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. Packet delivery in adhoc networks is achieved through routing and packet forwarding. So we should provide security for both operations. We provide an Efficient Security Framework (ESF) that protects both routing and data forwarding operations. Our framework involves (i) Detection of malicious nodes by the modified AODV protocol. (ii) Isolation of malicious nodes by using Multi-Signature based tickets. Through both analysis and simulation results, we demonstrate the effectiveness of our framework in a highly mobile and hostile environment.

Key words:
AODV protocol, wireless personal area networks, Attacks, Detection, RREQ Flooding

1. Introduction

Wireless networking technologies are increasingly penetrating into everyday life. Examples of successful technologies such as the IEEE 802.11 family of wireless Local Area Network (WLAN) protocols, and bluetooth for Personal Area Networks (WPANs), are intended to provide the flexibility of forming networks in an ad hoc manner, without access to any infrastructure, or by extending a pre-existing network infrastructure, e.g. to provide access to a wired campus LAN and/or the internet. Recent developments also foresee WLAN technologies to be a complement to third generation mobile communication networks. The use of WLAN as radio access network in hot spot areas is seen as an approach to increasing network capacity, handling a larger number of users [1].

While WLANs have been focusing on high data rate and relatively long range applications, WPANs mainly target low data rate and short range applications1. IEEE 802.15.4-2003 (Low Rate WPAN) deals with low data rate but very long battery life (months or even years) and very low complexity. The first edition of the 802.15.4 standard was released in May 2003. In March 2004, after forming Task Group 4b, task group 4 put itself in hibernation.

Manuscript received July 5, 2008.
Manuscript revised July 20, 2008.

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end user-oriented approaches, such as Wi-Fi). The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more [2].

The basic framework conceives a 10-meter communications area with a transfer rate of 250 kbit/s. Tradeoffs are possible to favor more radically embedded devices with even lower power requirements, through the definition of not one, but several physical layers. Lower transfer rates of 20 and 40 kbit/s were initially defined, with the 100 kbit/s rate being added in the current revision.

Even lower rates can be considered with the resulting effect on power consumption. As already mentioned, the main identifying feature of 802.15.4 among WPAN's is the importance of achieving extremely low manufacturing and operation costs and technological simplicity, without sacrificing flexibility or generality.

In This paper we analyze the threats countered by LR-WPANs with respect to the protocol stack defined by IEEE 802.15.4 [1] and the ZigBee Alliance [3]. We have also modeled the attacks and evaluated their impacts also. Then we have identified some security problems within the current LR-WPAN security architecture and we have given some solution. We have also presented countermeasures of various attacks.

In this paper we analyze the threats countered by LR-WPANs with respect to the protocol stack defined by IEEE 802.15.4 [2] and the ZigBee Alliance [3]. We have also modeled the attacks and evaluated their impacts also. Then we have identified some security problems within the current LR-WPAN security architecture and provided an efficient security framework (ESF) that protects both routing and data forwarding attacks. The framework involves Detection of malicious nodes by the modified AODV routing and isolation of malicious nodes by using multi-signature based tickets.

The rest of the paper is organized as follows. In Section II, we survey the related work in this security area. In Section III, we present the overview of LR-WPANS with its different routing protocols,. In sections IV we describe the threats faced by LR-WPANs. In section V & VI, we describe our proposed algorithms for detection and isolation of malicious nodes, respectively. Section VII gives the simulation results and this paper is finally concluded in Section VIII.

2. Related work

Jianliang Zheng and Myung J. Lee [4] present a few application scenarios to show the potential extent to which the new standard can affect our lives, and then give an overview of the standard, focusing on its feasibility and functions in establishing ubiquitous networks and then also outline some quantitative results from their experiments so as to have a better view of the standard.

Charles E.Perkins and Elizabeth M.Royer[5] gives Ad-hoc on Demand Vector Routing(AODV),a novel algorithm for the operation of such ad-hoc networks and they show that their algorithm sales to large populations of mobile nodes wishing to form ad-hoc networks.

Ian D. Chakeres and Luke Klein-Berndt [6] have described AODVjr, a simplified version of the AODV protocol and this AODVjr is compared in simulation to a full featured AODV implementation and their results show that AODVjr performs as well as AODV and describes other positive effects of a smaller protocol specification.

Lidong Zhou and Zygmunt J. Haas [7] discussed the threats an ad hoc network faces and the security goals to be achieved and they identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication and also they use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.

Greg O'Shea and Michael Roe [8] found a unilateral authentication protocol for protecting IPv6 networks against abuse of mobile IPv6 primitives and their protocol integrates distribution of public keys and protects against falsification of network addresses and this is easy to implement, economic to deploy and lightweight in use.Their protocol is intended to enable experimentation with (mobile) IPv6 before the transition to a comprehensive IPSEC infrastructure.

JeanPierre Hubaux, Levente Butty´an and Srdan C apkun[9] provides an overview of security problems for mobile ad hoc networks,distinguishing the threats on basic mechanisms and on security mechanisms and then describes their solution to protect the security mechanisms.

Dalit Naor,Moni Naor and Jeff Lotspiech[10] discussed the problem of a center sending a message to a group of users such that some subset of the users is considered revoked and should not be able to obtain the content of the message and present a framework called the Subset-Cover framework, which abstracts a variety of revocation schemes including some previously known onesand also they describe two explicit Subset-Cover revocation algorithms; these algorithms are very flexible and work for any number of revoked users.

Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar [11] presents a set of Security Protocols for Sensor Networks, SPINS. The chief contributions of this paper are: Exploring the challenges for security in sensor networks, providing authenticated streaming broadcast, Designing and developing SNEP (Secure Network Encryption Protocol) providing data confidentiality, two-party data authentication, and data freshness, with low overhead and Designing and developing an authenticated routing protocol using SPINS building blocks.

Adrian Perrigy_Ran Canettiz Dawn Songy J. D. Tygar [12] proposes several substantial modifications and improvements to TESLA. One modification allows receivers to authenticate most packets as soon as they arrive. Other modifications improve the scalability of the scheme, reduce the space overhead for multiple instances, increase its resistance to denial-of-service attacks, and more.

Adrian Perrig,Dawn Song and J. D. Tygar[14] have designed and implemented ELK, a novel key distribution Protocol and they design a member join protocol that does not require any broadcast but requires that the server computes a oneway function on all keys in each time interval.

JeanPierre Hubaux, Levente Butty´an and Srdan C˘ apkun[15] provides an overview of security problems for mobile ad hoc networks,distinguishing the threats on basic mechanisms and on security mechanisms and then describes their solution to protect the security mechanisms.

Yih-Chun Hu, David B. Johnson and Adrian Perrig[17] evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV) and they present the design and evaluation of a new secure ad hoc network routing protocol using distance vector routing.

Baruch Awerbuch, David Holmer, Cristina NitaRotaru and Herbert Rubens[18] proposes an on-demand routing protocol for ad hoc wireless networks that provides resilience to byzantine failures caused by individual or colluding nodes and their adaptive probing technique detects a malicious link after log n faults have occurred, where n is the length of the path.

Seung Yi, Prasad Naldurg and Robin Kravets[19] developed a new routiong technique called Security Aware ad hoc Routing(SAR) that incorporates security attributed as parameters into ad hoc route discovery and they develop a two-tier classification of routing protocol security metrics.

Chris Karlof and David Wagner [20] have proposed security goals for routing in sensor networks,show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks,introduce two classes of novel attacks against sensor networks—sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols and they describe crippling attacks against all of them and suggest countermeasures and design considerations.

Vikram Srinivasan, Carla F. Chiasserini, Pavan Nuggehalli, Ramesh R. Rao[21] address the problem of providing traffic quality of service and energy efficiency in ad hoc wireless networks and they present a primal formulation of the problem,which uses penalty functions to take into account the system constraints, and we introduce a new methodology for solving the problem.

Chung Kei Wong [22] presents three strategies for securely distributing rekey messages after a join/leave and specify protocols for joining and leaving a secure group and they show that their group key management service, using any of the three rekeying strategies, is scalable to large groups with frequent joins and leaves.

Chris Karlof, Yaping Li, Joseph Polastre [23] have proposed ARRIVE, a probabilistic algorithm that leverages the high node density and the inherent broadcast medium found in sensor networks to achieve routing robust to both link failures and patterned node failures and they have found that ARRIVE adapts to large patterned failures within a relatively short period of time at the cost of only moderate increases in overall power consumption and source-to-sink latency.

3. An Overview of LR-WPANS

3.1 A Functional Overview of Network Layer

Routing is the major task of Network layer. Currently the ZigBee Alliance [3] is using an integrated routing, which has been proposed by the authors of [24]. The integrated routing is the combination of cluster-tree routing and AODV Junior (AODVjr) [6] routing. A brief description of the cluster-tree routing and the integrated routing as per [24] is given in the next paragraphs.

3.1.1 Cluster-Tree Routing

Through the association primitive supported by 802.15.4, a logical tree, referred to as cluster-tree, can be formed along with the setup of an LR-WPAN. The first node in a PAN will designate itself as the PAN coordinator and begin to accept association requests from other nodes. Any node already in the PAN can determine whether to allow other nodes to join it, that is, whether to act as a coordinator, depending on the availability of its resources such as memory and energy. In a cluster-tree, a node is able to calculate the next hop by looking at the destination address in the packet. This precludes the need of route discovery, and thus helps reduce the initial latency, control overhead, memory consumption and energy consumption.

In the cluster-tree, a node can have a maximum number of *Cm* children and a node can be at most *Lm* levels (i.e. hops) away from the root of the tree (*Cm* and *Lm* are two predetermined network-wide constants). A node with a short address *s* is in charge of assigning short addresses to its children according to the following algorithm: assign short address *s*+1 to the first child, *s*+1+*Cskip* (*Ls*) to the second child, and *s* + 1 + (*n ¡* 1) *Cskip* (*Ls*) to the *nth* child, up to the (*Cm*) *th* child. And *Cskip* (*Ls*) is calculated as follows:

$$C_{skip}(L_s) = \left\lfloor \frac{B - \sum_{k=0}^{L_s}(C_m)^k}{(C_m)^{L_s+1}} \right\rfloor$$

where *B* is the address block size of the whole network and *Ls* is the level of the node. For a full block, *B* can be calculated using *Cm* and *Lm* as follows:

$$B = \sum_{k=0}^{L_m}(C_m)^k$$

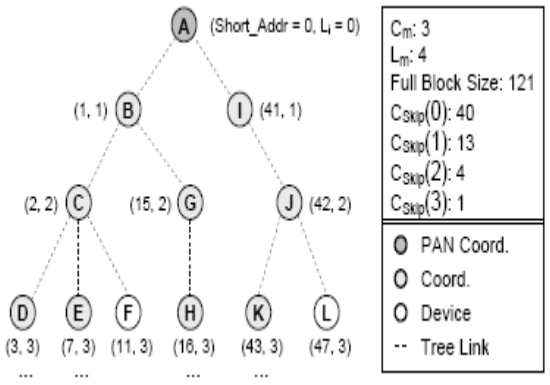

Fig. 1 A Cluster Tree Example

Fig. 1 is an example of cluster-tree with *Cm* = 3 and *Lm* = 4. Node *A* is the PAN coordinator with a short address 0. Since *Cskip*(0) = 40, node *A* assigns the short addresses 1 and 41 to its two children *B* and *I* respectively. Similarly, node *B* assigns the short addresses 2 and 15 to its two children *C* and *G* respectively, using *Cskip*(1) = 6. This procedure continues until the network reaches the maximum *Lm* levels. Some branches may terminate at a level less than *Lm* if the nodes at the end of those branches (e.g., node *F* and *L* in Fig. 2) stop supporting associations. Now suppose a node *S* with a short address *s* needs to relay a packet destined for node *Z* with a short address *z*. If $s < z \leq s + C_{skip}(L_s) \times C_m$ the packet will be relayed to the child with short address $s + 1 + c_i * C_{skip}(L_s)$ where $c_i = \left\lfloor \frac{z-s-1}{C_{skip}(L_s)} \right\rfloor$. otherwise, the packet will be relayed to the parent of node *S*.

3.1.2 Integrated Routing

In the integrated routing, a node falls into one of the following two classes: (1) routing node plus (RN+), which has enough memory to perform AODVjr routing; (2) routing node minus (RN-), which has limited memory and only performs cluster-tree routing. While an RNnode always follows the cluster-tree, an RN+ node can either follow the cluster-tree or dynamically discover an AODV route, depending on various factors such as session duration and tolerable route discovery delay. Cluster-tree routing favors memory-constrained devices and is very suitable for short communication sessions. With the cluster-tree, a device can immediately begin to transmit packets to other devices once it joins the network, without going through the route discovery procedure. However, as we can see from Fig. 1, most cluster tree routes are not optimal in terms of hop count. Cluster-tree routing also results in uneven traffic distribution. That is, a node at a smaller level normally needs to handle more traffic than a node at a larger level. As such, a node at a smaller level dies more quickly than other nodes due to its quick battery depletion. Without other mechanisms, single point of failure (SPOF) and network partition could easily happen in such a network. AODV and AODVjr, on the other hand, are capable of finding optimal or near-optimal routes, and thus help reduce the message delivery latency. Nevertheless, compared with cluster-tree routing, they require more memory to store routing entries and also incur much control overhead. As most routes are formed on demand, the initial latency caused by route discovery is high. In general, AODV and AODVjr are suitable for devices with sufficient memories, and favor long communication sessions. The integrated routing combines these two routings and makes tradeoff between them according to the network conditions and requirements.

4. Threats Faced By LR-WPANS

Security in wireless networks has become an active research area in recent years. Much related research work has been done for both wireless mobile ad hoc networks and wireless sensor networks, including key management [7] authentication [11], [12], [13], [14], [15], secure routing [16], [17], [18], [19], [20], cooperation and unfairness [21]. With the proliferation of LR-WPANs, the availability of security services for those networks will become a key issue. In the following subsections, we first present the general security objectives we want to pursue. And then we identify some types of attacks in the context of LR-WPANs

4.1 Security Objectives

Confidentiality: The assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality is critical to total data security. Encrypting data by using digital certificates and the Secure Socket Layer (SSL) helps ensure confidentiality when transmitting data across untrusted networks. Your security policy should address how you will provide confidentiality for information within your network as well as when information leaves your network [25] .

Integrity: The assurance that arriving information is the same as what was sent out. Understanding integrity requires you to understand the concepts of data integrity and system integrity.

Authentication: The assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access

a system. Traditionally, systems have used passwords and user names for authentication

Freshness: Unlike most general purpose networks, LRWPANs are normally task specific. Information flowing in an LR-WPAN is often time-sensitive. In such networks, it is not enough to only guarantee confidentiality and authentication. Replaying stale (but secret and authentic) messages can substantially disrupt the network operations and even cause catastrophes. Freshness ensures that the received message is recent and valid in the context of the applications.

Availability: meaning that the assets are accessible to the authorized parties in a timely manner (as determined by the systems requirements). The failure to meet this goal is called a denial of service.

Fairness: Fairness ensures that the network resources are used in a fair and efficient way.

Non-repudiation: Non-repudiation is proof that a transaction occurred, or that you sent or received a message. The use of digital certificates and public key cryptography to "sign" transactions, messages, and documents supports non-repudiation. Both the sender and the receiver agree that the exchange took place. The digital signature on the data provides the necessary proof.

Authorization: The assurance that the person or computer at the other end of the session has permission to carry out the request. Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Usually, authorization is performed in context of authentication.

Resource protection: Your resource protection scheme ensures that only authorized users can access objects on the system. The ability to secure all types of system resources is an iSeries strength. You should carefully define the different categories of users that can access your system. Also, you should define what access authorization you want to give these groups of users as part of creating your security policy.

4.2 Network Layer Attacks

It is a big challenge for a Network layer routing protocol to function correctly and efficiently in the presence of Byzantine attacks which attempt to disrupt the routing service. Routing attacks can generally be characterized into the following types: routing disruption and resource consumption. These two types of attacks can be launched against both the cluster-tree and AODVjr, the two components of the integrated routing. Here we only give out some attack examples aimed at the clustertree, since attacks aimed at AODVjr and other popular wireless routings have been addressed in many literatures [16], [17], [18], [19], [20]. Misuse goals are listed as follows [26].

- Route Disruption (RD). Route Disruption means either breaking down an existing route or preventing a new route from being established.
- Route Invasion (RI). Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.
- Node Isolation (NI). Node isolation refers to preventing a given node from communicating with any other node in the network. It di ers from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.
- Resource Consumption (RC). Resource consumption refers to consuming the communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.

There may be other attack goals (e.g., denial of service); however, we do not consider them in our current work.

To facilitate the analysis, we further classify misuses of the AODV protocol into two categories: atomic misuses and compound misuses. Intuitively, atomic misuses are performed by manipulating a single routing message, which cannot be further divided. In contrast, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol. It is easy to see that atomic misuses may be used as building blocks of compound misuses.

We perform our analysis of atomic misuses through understanding the effects of possible atomic misuse actions. Each atomic misuse action is an indivisible manipulation of one routing message. Specially, we divide the atomic misuse actions in AODV into the following four categories:

- Drop (DR). The attacker simply drops the received routing essage.
- Modify and Forward (MF). After receiving a routing message, the attacker modi_es one or several_elds in the message and then forwards the message to its neighbor(s) (via unicast or broadcast).
- Forge Reply (FR). The attacker sends a faked message in response to the received routing message. Forge Reply is mainly related to the misuse of RREP messages, which are in response of RREQ messages.
- Active Forge (AF). The attacker sends a faked routing message without receiving any related message.

5. Security Scheme for AODV

5.1 DoS Attack Due to RREQ Flooding

In AODV, a malicious node can override the restriction put by RREQ_RATELIMIT [5] (limit of initiating / forwarding RREQs) by increasing it or disabling it. A node can do so because of its self-control over its parameters. The default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. A compromised node may choose to set the value of parameter RREQ_RATELIMIT to a very high number. This allows it to flood the network with fake RREQs [5] and lead to a kind of DoS attack. In this type of DoS attack a non-malicious node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs. This leads to the following problems:

- Wastage of bandwidth
- Wastage of nodes' processing time (more overhead)
- Exhaustion of the network resources like memory (routing table entries)
- Exhaustion of the node's battery power

This further results in degraded throughput. Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication. This implies that the existing version of AODV is vulnerable to such type of malicious behavior from an internal node (which is then termed as a compromised node).

5.2 Proposed Scheme

5.2.1. Overview

In our proposed solution, we solve the problems caused due to flooding of RREQs from a compromised node. A compromised node may send large number of fake RREQ packets per second. In the proposed scheme, this can be checked by the node's neighbor, thus ensuring the compliance of this restriction.

5.2.2. Detection Of Malicious Nodes

In our proposed solution, we keep two counters: ACCEPT _THRESHOLD and BLACKLIST _THRESHOLD. RREQs upto this threshold value are accepted and processed by a node per unit time. Whenever the RREQs exceeds this threshold, they are dropped by recording their timestamp value. This information will aid in monitoring the neighbor's activities. During the simulation, we can set any value for this counter or it can be made adaptive, depending upon node metrics such as it memory, processing power, battery, etc.

The BLACKLIST_THRESHOLD counter is used to determine a malicious node. For this, first we have to count the number of RREQs originated/forwarded by a neighboring node per unit time. If this count exceeds the BLACKLIST_THRESHOLD, we can assume that the corresponding neighboring node is a malicious node which is trying to flood the network by sending possibly fake RREQs. After identifying a malicious neighboring node, it is added into the list of malicious nodes to prevent further flooding of the fake RREQs in the network. On detecting a malicious node, an attack notification (AN) packet containing its id, is broadcast to all other nodes to prevent further flooding of the fake RREQs in the network. By blacklisting a malicious node, all neighbors of the malicious node restrict the RREQ flooding and are therefore free to admit the RREQs from other genuine nodes.

Nodes that are confident about the malicious nature of a particular node, can avoid using it for subsequent network functions. In this way genuine nodes are saved from experiencing the DoS attack.

6. Isolation of Malicious Nodes

6.1. Network Design

We consider a special-purpose PAN consisting of N nodes with M authorized servers. The network size N may be dynamically changing with node join, leave, or failure over time. Each node A has a unique ID, denoted by IDA and assumed to be its network-layer address as usual. Each node maintains a reliability index list (RIL) of all nodes. Let {rl1,rl2,…..rln} denotes the initial reliability index of all nodes.

A secret key K is divided into M shares and stores one share at one authorized servers. Each node must possess a valid ticket in order to interact with other nodes and participate in the network. The ticket contains the following fields owner id, a timestamp ts , expiry time es. The authorized servers using multiple-key concepts issue this ticket. If a node wants its ticket signed by the authorized server, it sends the request message to one of the servers.

Each authorized server signs the ticket with its share in turn, and the last authorized nodes sends the ticket to the requested node. Since every authorized server is required to generate the valid signature, even if a malicious node has many identities among the authorized node group, it cannot forge signatures when there are good authorized servers.

The ticket is signed and issued by a group of nodes while no single node can do so and each node renews the ticket when its current ticket expires. The ticket of the convicted

malicious node will be revoked. The process of ticket renewal and revocation is discussed in section B.

6.2. Ticket Renewal and Revocation

Before the current token expires, each node requests its local neighbors to renew its ticket. The node that needs ticket renewal broadcasts a renewal request (RENREQ) packet, which contains its current ticket and a timestamp.

When a node receives a RENREQ packet, the RIL is used to decide whether to serve the request or not. Specifically, when a node receives a RENREQ packet from its neighbor, it extracts the ticket from the packet. It checks whether the ticket has already been revoked by comparing it with the RIL. If the ticket is still valid yet about to expire, it constructs a new token with owner id equal to that in the old ticket, equal to the timestamp in the RENREQ packet. The expiry time is determined by the reliability index of that node. It then signs the newly constructed ticket using its own share of K, encapsulates the partially signed ticket in a renewal reply (RENREP) packet, and then unicasts the RENREP packet back to the node from which it received the RENREQ packet. RENREQ packets containing revoked tickets are silently dropped. When the requesting node receives RENREP packets from different neighbors, it combines these partially signed tickets into a single ticket signed with K.

Now, we describe how a malicious node's ticket is revoked in the network. Recall that each node keeps a reliability index list (RIL) of all nodes. Whenever a node receives an AN packet against a malicious node, it decreases the reliability index of that node by 1. If the reliability index decreases below a pre-defined threshold rmin, it constructs a notification of ticket revocation, signs the notification using its own share of K, and then broadcasts the notification. Because only nodes with valid tokens can participate in the network operations, the token revocation mechanism ensures that a malicious node is isolated right after it was detected. The blacklisted node is isolated from the other nodes for a period of time B1. If the blacklisted node continues its malicious activitity for the next B1 period, then we fix B1 = B1 * 2 for that node.

Our Detection and Isolation scheme can be summarized as follows:

Algorithm

1. Let $\{n_i , i=1,2,\ldots\ldots N\}$ be the nodes in the network
   Let $\{rl_i , i=1,2 . \ldots\ldots N\}$ be the Reliability index of each node
2. Calculate the reliability index
   $rl_i = N , i = 1,\ldots\ldots N$
3. Each node broadcast its reliability index to all nodes and $\{RIL_i, i=1,2 . \ldots\ldots N\}$be the Reliability index list stored in each node
4. Let *a* be the attacker .
5. for $\{ R_i \}, i=1,2,\ldots..N$
   {
   if (R_i detects *a*) then
   R_i broadcast AN_a, where AN_a , Attack Notification Packet = id_a.
   if (n_i receive AN_a) then
   $rl_a = rl_a - 1$
   endif
   endif
   }
6. Let rlT be the reliable threshold of a node.
7. Let et_i be the expiry time of the ticket of node n_i.
8. if($et_i > ct$) then
   generate the renewal request $RENREQ_i$.
   endif
9. n_i broadcast $RENREQ_i$ to $\{nd_{i,j}\}$,
   where $\{nd_{i,j}\}$, j=1,2…k for all k neighbors of n_i .
10. On receiving $RENREQ_i$, each $nd_{i,j}$ check the condition.
    If ($rl_i < rlT$), then
    reject $RENREQ_i$.
    else
    generate the renewal reply $RENREP_i$.
    $nd_{i,j}$ unicast $RENREP_i$ to n_i .

6.2.1. Advantages of the Proposed Scheme

- There is no extra overhead in implementing our proposed scheme in the existing version of AODV.
- The proposed scheme is more efficient in terms of its resource reservations and its computational complexity.
- Our proposed scheme can also be applied in the case of more than one malicious node.

7. Simulation Results

In this section, we evaluate the performance of our proposed framework (ESF) through extensive simulations. We have implemented ESF in the ns-2 simulator. Our performance evaluations are based on the simulations of 50 wireless nodes that form a LR-WPAN over a rectangular (50Mx50m) flat space in 100s of simulation time. The MAC layer protocol and the routing protocol are 802.11 DCF and AODV protocol, respectively.

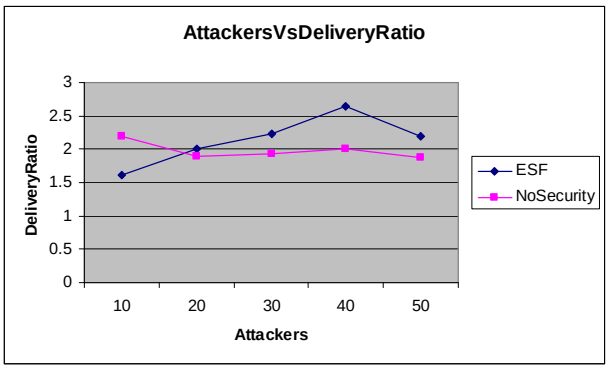

Fig. 2 Attackers Vs Delivery Ratio

In case (i), we study the performance of No of attackers vs. Packet delivery ratio. We vary the attackers as 10,20,…50 . The results are shown in Fig.(1) , from which we can observe that , the delivery ratio is mush better than that of no security scenario.

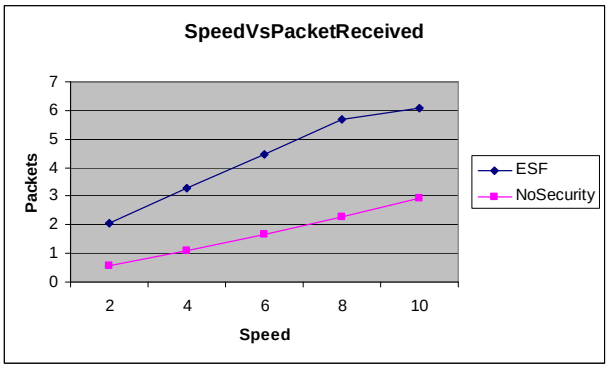

Fig. 3 Node Speed Vs Packets Received

In case(iii), we study the performance of Node speed vs. Packet received. We vary the speed as 2,4,6…10. The results are shown in Fig.(2) , from which we can observe that , the packets received is mush better than that of no security scenario.

8. Conclusion

In This paper we have analyzed the threats countered by LR-WPANs with respect to the protocol stack defined by IEEE 802.15.4 and the ZigBee Alliance. We have also modeled the attacks and evaluated their impacts also. Then we have identified some security problems within the current LR-WPAN security architecture and provided an efficient security framework (ESF) that protects both routing and data forwarding attacks. The framework involves Detection of malicious nodes by the modified AODV routing and isolation of malicious nodes by using multi-signature based tickets. Detection of malicious node is performed by each node by monitoring the RREQ packet forwarding activity of its neighbors. Then we have presented the ticket renewal and revocation mechanism using the combined signatures of multiple authorized servers. Through extensive simulation results, we demonstrate the effectiveness of our framework.

In future work, we will be concentrating on providing the data security and reducing the overhead of our framework.

References

[1] "Wireless Netwroking Technologies" From http://wln2003 .cs.bonn.edu/.
[2] "IEEE802.15.4" From http://en.wikipedia.org/wiki/IEEE 802.15.4
[3] ZigBee Alliance. http://www.zigbee.org.
[4] J. Zheng and M. J. Lee,"Will IEEE 802.15.4 make ubiquitousnetworking a reality? – A discussion on a potential low power, low bit rate standard," IEEE Communications Magazine, Vol. 42, No. 6, pp. 140-146,.2004. 140-146, Jun. 2004.
[5] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on demand distance vector (AODV) routing," IETF RFC 3561, Jul. 2003.
[6] I. Chakeres and L. Klein-Berndt, "AODVjr, AODV simplified," ACM SIGMOBILE Mobile Computing and Communications Review, pp. 100- 101, Jul. 2002.
[7] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Networks Special Issue on Network Security, Nov./Dec. 1999.
[8] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," ACM Computer Communications Review, vol.31, pp.4–8, July 2001.
[9] Jean-Pierre Hubaux, Levente Buttyan, Srdan Capkun, *The Quest for Security in Mobile Ad Hoc Network*s, ACM Symposium on Mobile Networking and Computing, MobiHOC 2001.
[10] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In Advances in Cryptology - CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139. 41–62. 2001
[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: Security protocols for sensor networks," In Wireless Networks Journal (WINE), Sept. 2002.
[12] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," In Network and Distributed SystemSecurity Symposium, NDSS 01, pages 35-46, Feb. 2001.
[13] A. Perrig, R. Canetti, D. Song, and D. Tygar, "The TESLA broadcast authentication protocol," In RSA Cryptobytes, summer 2002.
[14] A. Perrig, D. Song, and D. Tygar. Elk, a new protocol for efficient large-group key distribution. In Proc. of IEEE Symposium on Security and Privacy. 2001.
[15] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," In Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing 2001, Long Beach, CA.

[16] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," MobiCom, Atlanta, Georgia, Sept. 2002.
[17] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," In Proc. of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, Jun. 2002.
[18] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An ondemand secure routing protocol resilient to Byzantine failures," In ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, Sept. 2002.
[19] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad-hoc routing for wireless networks," MobiHOC Poster Session, 2001.
[20] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," In First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.
[21] V. Srinivasan, P. Nuggehalli, C-F. Chiasserini, and R. R. Rao, "Optimal rate allocation and traffic splits for energy efficient routing in ad hoc networks," In Proc. of Infocom 2001, New York City, Jun. 2001.
[22] C. Wong, M. Gouda,S. Lam. Secure Group Communication Using Key Graphs. In Proc. Of SIGCOMM'98, 1998.
[23] C. Karlof, Y. Li, and J. Polastre. ARRIVE: Architecture for Robust Routing In Volatile Environments. Technical Report UCB/CSD-03-1233, University of California at Berkeley, Mar. 2003.
[24] Jianliang Zheng, Myung J. Lee, Michael Anshel, "Towards Secure Low Rate Wireless Personal Area Networks" In IEEE TRANSACTIONS ON MOBILE COMPUTING.
[25] "Security policy and objectives" from http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzaj4/ rzaj4rzaj40j0securitypolco.htm.
[26] Peng Ning and Kun Sun "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols" Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society June 2003

Mrs.S.Padma Priya received her BE (Electronics and Commun- ication) from Madras University in the year 1991. and M.Tech(Information Techn-ology) from Punjab University and M.E.(Embeded Systems) from Anna University. She has been the member for evaluation committee for projects and served has Resource coordinator for Bharathdasan University and IGNOU. She has published papers in many national level conferences on embedded systems. She is now presently heading over the Information Technology Department in Prathyusha Institute of Technology and Management.

Mr. Jayaram Pradhan is the active member of Bherampur University, orissa. He is serving has Head of the Department on Computer Science Department. He has published many papers in International Seminar's in the fields' of Network Security. He has also guided over many doctorates in the field of Computer Science.