International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 11, November - 2013

Providing Security to Data Transmission over Wireless Sensor Network

Mr. Vicky G. Saokar
Dr. V. B. Kolte COE Malkapur

Prof. Lokesh Bijole
Dr. V. B. Kolte COE Malkapur

ABSTRACT

Wireless sensor networks are new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. When wireless sensor networks are deployed in a hostile terrain, security becomes extremely important, as they are prone to different types of malicious attacks. Due to the inherent resource limitations of sensor nodes, existing network security methods, including those developed for Mobile Ad-Hoc Networks, are not well suitable for wireless sensor networks. As a crucial issue security in wireless sensor networks have attracted a lot of attention in the recent year. This paper made a thorough analysis of the major security issue and presented the on-going aspect of further development to designers in their struggle to implement the most cost effective and appropriate method of securing their network.

1. INTRODUCTION

Wireless sensor networks are a new type of networked systems. Wireless nodes and is used in a variety of applications such as military sensing and tracking, environmental monitoring, disaster management, etc. Due to the nature of the military, it is obvious that the data is of a private nature and is required to remain this way to ensure the success of the application. Enemy tracking and targeting are among the most useful applications of wireless sensor networks in military terms. Characterized by severely constrained computational and energy resources. [1] When the wireless sensor networks are implemented in open, un-monitored hostile terrain, security becomes extremely important because different of malicious attacks. It is main issue security in wireless sensor networks has attracted a lot of attention in the recent year Nowadays, there is a growing interest in Wireless Sensor Networks WSNs are multiple mesh networks made of lots of small battery-powered sensors that generate data about the environment. in the Moreover, they set wireless communication capabilities allowing them to exchange data. The low capabilities of the sensors, their wireless communications, and the fact that they are deployed in open areas make them attract to attacks. Routing is a important issue in WSNs. Here, we consider a routing scheme called converge cast routing. In this problem, a node is distinguished as the sink and all non-sink nodes, called source nodes, must be able to transmit data to the sink on request. The sink can be arbitrary [3] far from other nodes. Importantly, in WSNs, source nodes are sensors and the sink is a base station that is linked to another network, like a gateway.

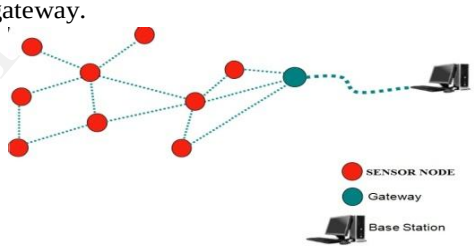

Figure 1.1: Wireless Sensor Network Architecture

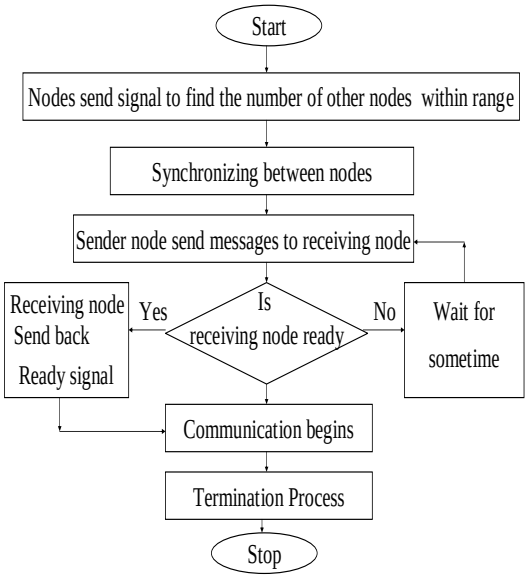

Figure 1.2: Working of a general Ad-Hoc Network

1.1. AD HOC ON-DEMND DISTANCE VECTOR (AODV)

Ad hoc On-Demand Distance Vector, AODV, is a distance vector routing protocol that is reactive. The reactive property of the routing protocol implies that it only requests a route when it needs one and does not require that the mobile nodes maintain routes to destinations that are not communicating [5, 6]. AODV guarantees loop-free routes by using sequence numbers that indicate how new, or fresh, a route is the AODV protocol is one of the on-demand routing protocols for ad-hoc networks which are currently developed by the IETF Mobile Ad-hoc Networks (MANET) working group. it follows the distance vector approach instead of source routing. In AODV, every node keeps a local routing table that contains the information to which of it neighbours it has to forward a data packet so that it reaches eventually the desired destination. [2] In general, it is desirable to use routes which have minimal length according to hop-count as a distance metric. However, AODV provides the functionality like DSR, namely to transport data packets from one node to another by finding routes and taking advantage of multiple hop communication. AODV is based on UDP as an unordered transport protocol to deliver packets within the ad-hoc network. Moreover, it requires that every node can be addressed by a network wide unique IP address and sends packets correctly by placing its IP address into the sender field of the IP packets. This means also that AODV is expected to run in a friendly network, where security is a minor concern. It should be mentioned that there are some attempts to extend AODV to prevent malicious nodes from attacking the integrity of the network by using digital signatures to secure routing control packets. AODV requires each node to maintain a routing table containing one route entry for each destination that the node is communicating with. Each route entry keeps track of certain fields. Some of these fields are:

a. **Destination IP Address**: The IP address of the destination for which a route is supplied.
b. **Destination Sequence Number**: The destination sequence number associated to the route.
c. **Next Hop**: Either the destination itself or an intermediate node designated to forward packets to the destination.
d. **Hop Count**: The number of hops from the Originator IP Address to the Destination IP Address.
e. **Lifetime**: The time in milliseconds for which nodes receiving the RREP consider the route to be valid.
f. **Routing Flags**: The stat of the route; up (valid), down (not valid) or in repair.

1.1.1 Route Discovery

Whenever a source node desires a route to a destination node for which it does not al-ready have a route, it broadcasts a route request (RREQ) message to all its neighbours. The neighbours update their information for the source and create reverse route entries for the source node in their routing tables.[3] A neighbours receiving a RREQ may send a route reply (RREP) if it is either the destination or if it has an unexpired route to the destination? If any of these two cases is satisfied, the neighbours uncast a RREP back to the source. Along the path back to the source, intermediate nodes that receive the RREP create forward route entries for the destination node in their routing tables. If none of the two cases mentioned is satisfied, the neighbours rebroadcast (forwards) the RREQ. Each mobile node keeps a cache where it stores the source IP address and ID of the received RREQs during the last PATH_DISCOVERY_TIM seconds. If a mobile node receives another RREQ with the same source IP address and RREQ ID during this period, it is discarded. Hence, duplicated RREQs are prevented and not forwarded. When searching for a route to the destination node, the source node uses the expanding ring search technique to prevent unnecessary network-wide dissemination of RREQs. This is done by controlling the value of the time to live (TTL) field in the IP header. The first RREQ message sent by the source has TTL=TTL_START. [9] The value of TTL defines the maximal number of hops a RREQ can move through the mobile ad hoc network, i.e. it decides how far the RREQ is broadcasted. In other words, it implies that the RREQ which is broadcasted by the source is received only by mobile nodes TTL hops away from the source (and of course all mobile nodes less than TTL hop away from the source). Apart from setting the TTL, the time-out for receiving a RREP is also set. If the RREQ times out without reception of a corresponding RREP, the source broadcasts the RREQ again. This time TTL is Incremented by TL_INCREMENT, i.e. the TTL of the second RREQ message is TTL_START + TTL_INCREMENT. This continues until a RREP is received or until TTL reaches TTL_THRESHOLD. If TTL reaches TTL_THRESHOLD a RREQ is sent

with TTL=NET_DIAMETER, which disseminate the RREQ widely, throughout the MANET. Broadcasting a RREQ with TTL=NET_DIAMETER is referred to as a network-wide search. If a source node does a network-wide search and still does not receive a RREP, it may try again to find a route to the destination node, up to a maximum of RREQ_RETRIES times.

1.1.2 Route Maintenance

When a link in a route breaks, the node upstream of the break invalidates all its routes that use the broken link. Then, the node broadcasts a route error (RERR) message to its neighbours (TTL is set to one). The RERR message contains the IP address of each destination which has become unreachable due to the link break. Upon reception of a RERR message, a node searches its routing table to see if it has any route(s) to the unreachable destination(s) (listed in the RERR message) which use the originator of the ERR as the next hop. If such routes exist, they are invalidated and the node broadcasts a new RERR message to its neighbours. This process continues until the source receives a RERR message. The source invalidates the listed routes as previously described and reinitiates the route discovery process if needed.

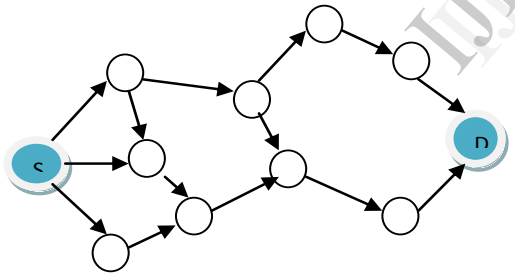

Figure 1.3: (a) Source node S initiates the path Figure 1.3: (b) A RREP sent back to the source.

Ad Hoc On-Demand Distance Vector routing protocol uses broadcast discovery mechanism, similar to but modified of that of DSR. To ensure that routing information is up-to-date, a sequence number is used. The path discovery is established whenever a node wishes to communicate with another, provided that it has no routing information of the destination in its routing table. Path discovery is initiated by broadcasting a route request control message "RREQ" that propagates in the forward path. If a neighbour knows the route to the destination, it replies with a route reply control message "RREP" that propagates through the reverse path. Otherwise, the neighbour will re-broadcast the RREQ. The process will not continue indefinitely, however, authors of the protocol proposed a mechanism known as "Expanding Ring Search" used by Originating nodes to set limits on RREQ dissemination. AODV maintains paths by using control messages called Hello messages, used to detect that neighbours are still in range of connectivity.

If for any reason a link was lost the node immediately engages a route maintenance scheme by initiating route request control messages. The node might learn of a lost link from its neighbours through route error control messages "RERR".

1.2. Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. A simple mechanism proposed to prevent the flooding attack in the AODV protocol. In his approach, each node monitors and calculates the rate of its neighbours' RREQ. If the RREQ rate of any neighbour exceeds the predefined threshold, the node records the ID of this neighbouring a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake. The authors show that a flooding attack can decrease throughput by 84 per cent. The authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. Similar to, in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the present time period. The RREQs

from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in, where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

2. LITERATURE SURVEY

This paper made a thorough analysis of the major security issue and presented the on-going aspect of further development to designers in their struggle to implement the most cost effective and appropriate method of securing their network. To resolve this problem the various algorithms are published for security to data transmission over wireless sensor network.

We propose SR3, a secure and resilient algorithm for converge cast routing in WSNs. SR3 uses lightweight cryptographic primitives to achieve data confidentiality and data packet enforceability. SR3Wemade simulations to show the resiliency of SR3 against various scenarios, where we mixed selective forwarding, black hole, wormhole, and Sybil attacks [1]. Routing is a crucial issue in WSNs. Here, we consider a routing scheme called *converge cast* routing. In this problem, a node is distinguished as the *sink* and all non-sink nodes, called *source nodes*, must be able to transmit data to the sink on request or according to an *a priori* unknown schedule.

2.1 Wormhole Attack

We also propose technique has been implemented with NS2 simulator over the DSR protocol. This technique for wormhole avoidance addresses the malicious nodes and avoids the routes having wormhole nodes without affecting the overall performance of the network. A wormhole attack [2] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. . Figure 2.1 shows an example of the wormhole attack against a reactive routing protocol.

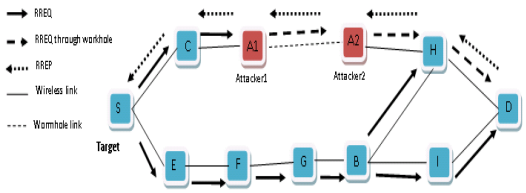

Figure 2.1: Wormhole attack on reactive routing

2.2 Black Hole attack

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure 2.2 shows an example of a black hole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

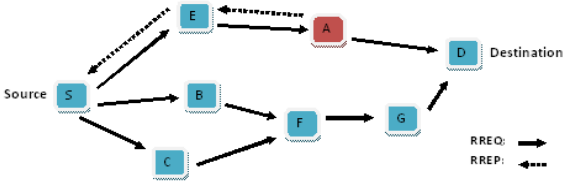

Figure 2.2: Black hole attack on AODV

The route confirmation request (CREQ) and route confirmation reply (CREP) is introduced in [3] to avoid the black hole attack.

3. PROBLEM DEFINITION

In the WSN most important part is security. A wireless sensor network is composed of tiny sensor nodes each capable of sensing some phenomenon, doing some limited data processing and communicating with each other [7]. These tiny sensor nodes are deployed in the target field in large numbers and they collaborate to form an adhoc network capable of reporting the phenomenon to a data collection point called sink or base station. These networked sensors have many potential civil and military applications i.e., they can be utilized for object tracking,

intrusion detection, habitat and other environmental monitoring related applications etc.

3.1 Coverage Holes

Although the coverage problem has been interpreted in a variety of ways in the existing literature, we follow [9] for defining the coverage hole problem as follows. Given a set of sensors and a target area, no coverage hole exists in the target area, if every point in that target area is covered by at least k sensors, where k is the required degree of coverage for a particular application.

3.2 Routing Holes

A routing hole consist of a region in the sensor network where either nodes are not available or the available nodes cannot participate in the actual routing of the data due to various possible reasons. These holes can be formed either due to voids in sensor deployment or because of failure of sensor nodes due to various reasons such as malfunctioning, battery depletion or an external event such as _re or structure collapse physically destroying the nodes.

3.3 Jamming Holes

An interesting scenario can occur in tracking applications when the object to be tracked is equipped with jammers capable of jamming the radio frequency being used for communication among the sensor nodes [10]. When this happens, nodes will still be able to detect the presence of the object in the area but unable to communicate the occurrence back o the sink because of the communication jamming.

4. PROPOSED ALGORITHAM

There are two primary motivations related with secured communication in MANETs. At first, secured communication evaluation helps discriminate between good and malicious entities. Creating secured history, one entity can remember others' behaviours. This memory provides a method for good entities to avoid working with (ex-villain) or suspect ones. Secondly, secured communication offers a prediction of one's future behaviour and improves network performance. The results of evaluation can be directly applied to a motivation for good or honest behaviours while a punishment for selfish or malicious behaviours in the network. The feedback reminds network participants to act more responsibly. These motivations have interested researchers from the areas of information security and computer network in secured communication of MANETs. And according to that secured communication system we eliminate the un-secured node and improve the performance of the network in MANET environment.

4.1. Assumptions

We consider arbitrary connected networks with bidirectional links, although we will focus on Unit Disk Graphs (UDG) in simulations. Each node p has a unique ID and knows the set of its neighbors, **Neigp** this latter assumption will be relaxed, when considering Sybil attacks. Networks are made of one sink, which is the data collector, and numerous source nodes. The source nodes are sensors, and consequently are limited in terms of memory, computational power, and battery. Sensors are non-trustworthy since they are vulnerable to physical attacks and an adversary can compromise them. In contrast, the sink is assumed to be robust and powerful in terms of memory, computation, and energy. So, we assume that it cannot be compromised. All nodes have access to a lightweight cryptography library(hash function, symmetric encryption, and secure random number generation). All source nodes share a symmetric key with the sink. Moreover, we assume that all source nodes have several data to route; however, the scheduling of the data generation is a priori unknown. Finally, there is no time synchronization between nodes.

4.2. Overview

Randomization is interesting to obtain resilient solutions because it generates behaviors unpredictable by an attacker. However, note that the "classical" uniform random talk, where a node chooses the next hop uniformly at random among its neighbors, is known to be inefficient even against small number of compromised nodes [12, 16]. So, we designed SR3 rather as a reinforced random walk, based on a reputation mechanism. The idea is to locally increase the probability of a neighbor to be chosen at the next hop, if it behaves well. Such a reputation mechanism is based on acknowledgments. We propose a scheme in which if a process receives a valid acknowledgment, it has the guarantee that the sink actually delivered the corresponding data message. Hence, upon receiving such an acknowledgment, a process cans legitimately increase its confidence on the neighbor to which it previously sent the corresponding data message. Therefore, eventually all honest nodes preferably choose their highly-reputed neighbors, and so the data messages tend to follow paths that successfully route data to the sink.

4.3 Power Consideration in Wireless Sensor Networks

The single most important consideration for a wireless sensor network is power consumption. While the concept of wireless sensor networks looks practical and exciting on paper, if batteries are going to have to be changed constantly, widespread adoption will not occur. Therefore, when the sensor node is designed power consumption must be minimized. Figure shows a chart outlining the major contributors to power consumption in a typical 5000-ohm wireless strain gage sensor node versus transmitted data update rate. Note that by far, the largest power consumption is attributable to the radio link itself [11].

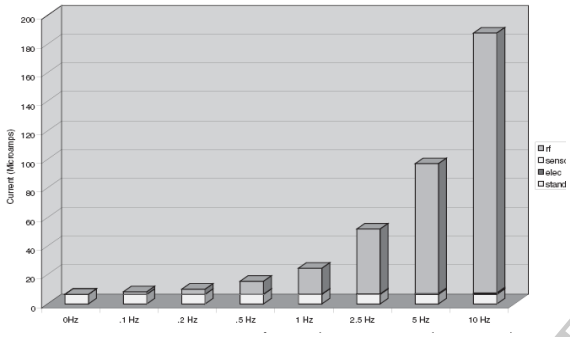

Figure 5.1: Power consumption of a 5000-ohm strain gauge wireless sensor node

There are a number of strategies that can be used to reduce the average supply current of the radio, including:

- Reduce the amount of data transmitted through data compression and reduction.
- Lower the transceiver duty cycle and frequency of data transmissions.
- Reduce the frame overhead.
- Implement strict power management mechanisms (power-down and sleep modes).
- Implement an event-driven transmission strategy; only transmit data when a sensor event occurs. Power reduction strategies for the sensor itself include:
- Turn power on to sensor only when sampling.
- Turn power on to signal conditioning only when sampling sensor.
- Only sample sensor when an event occurs.
- Sensor sample rate to the minimum required by the application.

4.4 Security Requirements

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to WSN.

4.4.1 Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following.

- A sensor network should not leak sensor readings to its neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g. key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.
- The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

4.4.2 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

4.4.3 Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed overtime. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related

counter, can be added into the packet to ensure data freshness.

4.4.4 Availability

The traditional encryption algorithms to fit within the wireless sensor network are not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.
- The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

4.4.5 Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every Self-Ealing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors. Several random key redistribution schemes have been proposed in the context of symmetric encryption techniques. In the context of applying public-key cryptography techniques in sensor networks, an efficient mechanism for public-key distribution is necessary as well. In the same way that distributed sensor networks must self-organize to support multihop routing, they must also self-organize to conduct key management and building trust relation among sensors. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

4.4.6 Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications etc. .The authors propose a set of secure synchronization protocols for sender-receiver (pair wise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

4.4.7 Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate no secured location information by reporting false signal strengths, replaying signals, etc. A technique called verifiable multi iterations (VM) is described in. In multi iteration, a device's position is accurately computed from a series of known reference points. Authenticated ranging and distance bounding are used to ensure accurate location of a node. Because of distance bounding, an attacking node can only increase its claimed distance from a reference point. However, to ensure location consistency, an attacking node would also have to prove that its distance from another reference point is shorter. Since it cannot do this, a node manipulating the localization protocol can be found. For large sensor networks, the SPINE (Secure Positioning for sensor NET works) algorithm is used. It is a three phase algorithm 8 based upon verifiable multi iteration. SeRLoc (Secure Range-Independent Localization) is described. Its novelty is its decentralized, range-independent nature. SeRLoc uses locators that transmit beacon information. It is assumed that the locators are trusted and cannot be compromised. Furthermore, each locator is assumed to know it's an own location. A sensor computes its location by listening for the beacon information sent by each locator. The beacons include the locator's location. Using all of the beacons that a sensor node detects, a node computes an approximate location based on the coordinates of the locators. Using a majority vote scheme, the sensor then computes an overlapping antenna region. The final computed location is the "centre of gravity" of the overlapping antenna

region. All beacons transmitted by the locators are encrypted with a shared global symmetric key that is pre-loaded to the sensor prior to deployment. Each sensor also shares a unique symmetric key with each locator. This key is also pre-loaded on each sensor.

4.4.8 Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle).[8] From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

5. PROPOSED SOFTWARE DISCRIPTION

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done usingNS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours .Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field .Among these are the University of California and Cornell University who developed the REAL network simulator,[12] the foundation which NS is based on. Since 1995 the Defence Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual Inter Network Test bed (VINT) project [9].2 currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile.

Main NS2 Simulation Steps

The followings show the three key step guideline in defining a simulation scenario in a NS2

Step 1: Simulation Design

The first step in simulating a network is to design the simulation. In this step, the users should determine the simulation purposes, network configuration and assumptions, the performance measures, and the type of expected results.

Step 2: Configuring and Running Simulation

This step implements the design in the first step. It consists of two phases: *Network configuration phase*: In this phase network components (e.g. node, TCP and UDP) are created and configured according to the simulation design. Also, the events such as data transfer are scheduled to start at a certain time. 2.6 A Simulation Example 27 *Simulation Phase*: This phase starts the simulation which was configured in the Network Configuration Phase. It maintains the simulation clock and executes events chronologically. This phase usually runs until the simulation clock reached a threshold value specified in the Network Configuration Phase In most cases, it is convenient to define a simulation scenario in a Tclscripting file (e.g., <file>) and feed the file as an input argument of an NS2

Invocation (e.g., executing “ns <file>”).

Step 3: Post Simulation Processing

The main tasks in this step include verifying the integrity of the program and evaluating the performance of the simulated network. While the first task is referred to as *debugging*, the second one is achieved by properly collecting and compiling simulation results.

6. APPLICATIONS

6.1 Structure Health Monitoring (SHM) System

SHM is another important domain for sensor network application. The combined US and Canada Civil infrastructure assets have an estimate value of US$25 trillion, SHM applications, serving as precaution measure, can have great social and economic impact. The widely accepted goals of SHM system include detecting damage, localizing damage, estimating the extent of the damage and predicting the residual life of the structure, as proposed in [11]. SHM has been an evolving technology since it was first proposed in

1990's, the latest approach, wireless sensor network based approach, is promising because it has many advantages: low deployment and maintenance cost, large physical coverage, high spacial resolution etc. One of the barriers is that damage detection is very difficult even for sophisticated sensors, thus breakthrough in damage detection using small
MEMS sensors is much needed. So far, a SHM system using wireless sensor network technology is yet to emerge.

6.2 Smart Energy

Societal-scale sensor network can greatly improve the efficiency of energy-provision chain, which consists of 3 components, the energy-generation, distribution, and consumption infrastructure. It is reported that 1 per cent load reduction due to demand response can lead to a 10 per cent reduction in wholesale prices, while a 5 per cent load response can cut the wholesale price in half. In the wake of recent energy regulation in California, proposes a gradual roll-out plan to make energy supply chain part of an integrated network of monitoring, information processing, controlling, and actuating devices, in a hope to spread the consumption of energy over time reducing peak demand. That would be a complex and long-term project.

6.3 Home Applications, Office Applications

This is a time that we witness more and more electronic appliances enter average household, great commercial opportunities exist in home automation, smart home/office environment. Given the great market potential, breakthrough in this section will surely mark a big milestone in sensor network research. An example application in this category is described in [12], Mani et al. present a .Smart Kindergarten. That builds a sensor-based wireless network for early childhood education. It is envisioned that this interaction-based instruction method will soon take place of the traditional stimulus-responses based methods.

7. CONCLUSION

Security in wireless sensor networks has attracted a lot of attention in the recent years. The severe energy constraints and demanding deployment environments of wireless sensor networks make computer security for these systems more challenging than for conventional networks. Components designed without security can easily become a point of attack. So it is critical to integrate security into every component to pervade security and privacy into every aspect of the design. According to using such technology we can fulfill our requirement that is providing security over wireless sensor network.

REFERANCES

[1] T. Eisenbarth and S. Kumar. A survey of lightweight-cryptographyimplementations. Design & Test of Computers, IEEE, 24(6):522–533,2007.

[2] R. Aleliunas, R. Karp, R. Lipton, L. Lovasz, and C. Rackoff. Randomwalks, universal traversal sequences, and the complexity of maze problems.In*20th Annual Symposium on Foundations of Computer Science*,pages 218–223, 1979.

[3] P.Bose, P. Morin, I. Stojmenovi´c, and J. Urrutia. Routing with guaranteed delivery in ad hoc wireless networks.*Wireless Networks,*7(6):609–616, 2001.

[4] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey on Attack andCountermeasures in Mobile ad hoc Networks", Dept. of computerscience and engineering, Florida Atlantic University, under reviewat Wiley Journal Wireless Communication and Mobile Computing(WCMC), 2006.

[7] R. Aleliunas, R. Karp, R. Lipton, L. Lovasz, and C. Rackoff. Randomwalks, universal traversal sequences, and the complexity of maze problems.In*20th Annual Symposium on Foundations of Computer Science*,pages 218–223, 1979.

[8] V. Mahajan , M. Natu , A.S. Sethi , "Analysis of Wormhole Intrusion Attack In MANETs", In proceedings of IEEE militarycommunication conference, 2008 IEEE.

[9] NICTA is funded through the Australian Government's *Backing Australia's Ability* initiative, in part through the Australian Research Council *Mobile Computing and Communications Review, Volume 1, Number 2*

[10] Ian F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, pages 102.114, 2002.

[11] Chi-Fu Huang and Yu-Chee Tseng. The coverage problem in a wireless sensor network. In *Proceedings of the 2nd ACM WSNA'03*, Sep 2003.

[12] Anthony D. Wood, John A. Stankovic, and Sang H. Son. JAM: A jammed-area mapping service for sensor networks. In *24th IEEE Real Time System Symposium (RTSS'03)*, pages 286.298, Dec 2003.

[13] Chris Townsend, Steven Arms MicroStrain, Inc. WilsonChapter22.indd 2004

IEEE International Conference on Distributed Computing in Sensor Systems 2013

[14] H. Kinawi, M. M. RedaTaha, and N. El-Sheimy. Gpsr: greedy perimeter stateless routing for wireless networks. In *27th Annual IEEE Conference on Local Computer Networks (LCN'02)*, 2002

[15] A. Rytter. Vibration based inspection of civil engineering structures, ph. d. dissertation, dept. of building technology and structural eng., aalborguniv., denmark. 1993.

[16] Mani B. Srivastava, Richard R. Muntz, and MiodragPotkonjak. Smart kindergarten: sensorbased wireless networks for smart developmental problem-solving enviroments. In *Mobile Computing and Networking*, pages 132.138, 2001

[17] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris. Resiliency of wireless sensor networks: Definitions and analyses. In Telecommunications \(ICT), 2010 IEEE 17th International Conference on, pages 828–835, 2010.