Observation on Finding & Resolving spiteful process in Wireless Sensor Networks

MaripiNayanappa Naidu[1] and P.Srilakshmi[2]

1. M.Tech. Degree in Computer Science Engineering, Avanthi Institute of Engineering and Technology. Vizianagaram, India
2. Associate Professor in the Department of Computer Science & Engineering at Avanthi Institute of Engineering and Technology. Vizianagaram, India

Abstract: *The main Objective of "Detecting Preventing Malicious Activities in Wireless Sensor Networks" is Preventing Malicious Activities in Wireless Sensor Networks. By Dynamic Random Password Generation and Comparison Method is used. Wireless sensor networks have many potential applications for both civil and military tasks, these days wireless sensor networks plays the major role in protection of network security. Major serious attacks of various kinds have been written in wireless sensor network till now by many researchers. The Sybil attack is a massive destructive attack against the sensor network where numerous genuine identities with forged identities are used for getting an illegal entry into a network. Discerning the Sybil attack, sinkhole, and wormhole attack while multicasting is a tremendous job in wireless sensor network. Basically a Sybil attack means a node which pretends its identity to other nodes. Communication to an illegal node results in data loss and becomes dangerous in the network. The existing method Random Password Comparison has only a scheme which just verifies the node identities by analysing the neighbours. A survey was done on a Sybil attack with the objective of resolving this problem. The survey has proposed a combined CAM-PVM (compare and match-position verification method) with MAP (message authentication and passing) for detecting, eliminating, and eventually preventing the entry of Sybil nodes in the network. Users request to implement a scheme of accurate security for wireless sensor network, to deal with the problems found. In this paper different Intrusion detection systems are analysed basis on design and performance in real time wireless sensor network environment.*

Keywords:*Wireless Networks, Intrusion Detection System, Malicious Activities, Prevention, Attacker Node, Random Password Generation, Sybil Attack, CAM-PVM*

Introduction:

The Wireless Sensor Networks (WSNs) are vulnerable to various kinds of security threats that can degrade the performance of the network and may cause the sensors to send wrong information to the sink. Key management, authentication and secure routing protocols cannot guarantee the required security for WSNs. Intrusion Detection System (IDS) provides a solution to this problem by analysing the network in order to detect abnormal behavior of the sensor node(s). Researchers have proposed various approaches for detecting intrusions in WSNs during the past few years. In this survey, we classify these approaches into three categories and discuss them in detail wireless sensor network (WSN) is a network of cheap and simple processing devices (sensor nodes) that are equipped with environmental sensors for temperature, humidity, etc. and can communicate with each other using a wireless radio device. Sensor networks need to become autonomous and exhibit responsiveness without explicit user or administrator action. The unattended nature of WSNs and the limited resources of their nodes make them susceptible to attacks. Any defensive mechanism that could protect and guarantee their normal operation should be based on autonomous mechanisms within the network itself. Intrusion detection is an important aspect within the broader area of computer security, in particular network security, so an attempt to apply the idea in WSNs makes a lot of sense. The architectures for (Intrusion Detection System) IDS in WSN are

network-based and host-based. A network-based IDS uses raw network packets as the data source. It listens on the network and captures and examines individual packets in real time. A host based IDS uses the local data on host as a source to find the anomalies. Intrusion detection systems must be able to distinguish between normal and abnormal activities in order to discover malicious attempts in time. There are three main techniques that an intrusion detection system can use to classify actions misuse detection, anomaly detection and specification based detection. In misuse detection or signature-based detection systems, the observed behavior is compared with known attack patterns (signatures). Action patterns that may pose a security threat must be defined and stored to the system. Anomaly detection systems focus on normal behaviors, rather than attack behaviors. First these systems describe what constitutes a "normal" behavior (usually established by automated training) and then flag as intrusion attempts any activities that differ from this behavior by a statistically significant amount. Finally, specification-based detection systems are also based on deviations from normal behavior in order to detect attacks, but they are based on manually defined specifications that describe what a correct operation is and monitor any behavior with respect to these constraints. To make the final decision that a node is indeed an intruder and actions should be taken. There are two approaches for this. Either we could use a cooperative mechanism or let nodes decide independently. In an independent decision-making system, there are certain nodes that have the task to perform the decision-making functionality. They collect intrusion and anomalous activity evidences from other nodes and they make decisions about network-level intrusions. In a cooperative IDS system, if a node detects an anomaly, or if the evidence is inconclusive, then a cooperative mechanism is initiated with the neighboring nodes in order to produce a global intrusion detection action. In this paper different IDS approaches in WSN are discussed on basis of Design and Performances parameters. The paper is organized as follows: Section 2 discusses the intrusion detection and decision making methodology used in different IDS's. Section 3 gives the idea about the system models of IDS's. Section 4 provides the analysis and evaluation of proposed IDS's and Section 5 concludes the paper. In this survey, we classify these approaches into three categories and discuss them in detail

Problem Statement:

Devices used under wireless networks mostly access internet based applications like reservation, enquiry, billing, online payment and online transaction etc. Since, most of the vulnerability appears via internet it is necessary to provide a security mechanism for communication elements. The main objective of this System is to design a mechanism for detecting malicious activity in terms of their Identity.

Complication of Sensor Security:

A wireless sensor network is a special network which has many constraints comparing to the other networks. These constraints make difficult to directly employ the existing security to the wireless sensor networks. The followings are the brief discussion on these constraints of a sensor network

Required Resources:

 Security approach requires a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

 Required Memory and Storage Space - A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type has an 8-bit, 4MHz CPU only with only 4.5K available disk. Due to such limitation, the security related code must also be quite small.

Inconstant Communication:

Inconstant communication is another key challenge to sensor security. The network security depends on network protocol, which in turn depends on communication.

 Inconstant Transfer - The packet-based routing of the sensor network is normally connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. If the protocol lacks of appropriate error handling, it is possible to lose critical security packets. This may include, for example, a cryptographic key.

 Conflicts - In a high-density sensor network if packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail which can be a major problem in providing security.

 Latency - The multi-hop routing, network congestion, and node processing can lead to the latency of the network, thus make it difficult to achieve the synchronization among sensor nodes. The synchronization issues can be critical to sensor security.

Abandoned Operation:

The sensor nodes may be left unattended for long periods of time for a particular sensor network. There are three main caveats to unattended sensor nodes as describe follow.

Exposure to Physical Attacks - The sensor may be deployed in an environment open to adversaries, bad weather, and so on. These sensors may suffer a physical attack in such an environment.

Managed Remotely - Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues. The longer that a sensor is left unattended the more likely that an adversary has compromised the node.

Security Requirements:

A sensor network also poses unique requirements of its own as well as shares some commonalities with a typical computer network. The factors related to the security of a sensor network are described below

Sensor Networks vs. Ad-hoc Wireless Networks:

Wireless sensor networks may appear similar to ad-hoc wireless networks, but several important distinctions can be drawn between the two.

 Ad-hoc networks typically support routing between any pair of nodes, whereas sensor networks have a more specialized communication pattern, like many-to-one, one-to-many and local communication.

 In most of the sensor networks nodes are not mobile, possibly embedded in walls or dispersed from an airplane in a filed.

 Sensor networks are more resource constrained in respect of ad-hoc networks. Nodes in an ad-hoc

network may have a 32-bit processor, megabytes of RAM, a 2 Mbps radio, and a large battery, whereas a typical sensor node have an 8-bit processor, kilobytes of RAM, a 40 Kbps radio, and a tiny battery.

 There may exists a significant amount of redundancy in sensor network traffic as an event in the environment may cause several neighboring nodes to send data to the sink at correlated times. This redundancy is almost absent in case of ad-hoc network

Literature Review:

As technology advances the use and popularity of Wireless Sensor Networks (WSN) have been growing. However, the network protocols associated with WSNs have primarily been designed for energy efficiency. In this paper we investigate the security mechanisms designed for each, the data-link, network and application layers. Through the review of recently publish material, this paper investigates the security vulnerabilities associated with data-aggregation, routing and user authentication in WSN environments. This paper finds that security is not properly implemented for any of these technologies, leaving WSNs open to a plethora of attacks. Wireless sensor networks have become a large area of research, with many universities and institutes contributing. There has been a large body of research on detection of coverage holes in WSNs over the last few years. In this section, some of the typical hole detection algorithms of each category is analysed and summarized. (J. Yang et.al, 2003) proposed a Hole Detection and Adaptive geographical Routing (HDAR) algorithm, which focuses on defining and detecting holes in ad hoc network, representing holes and building routes around the holes. It is based on the geographical approach. The contributions of this paper are threefold. First, a heuristic algorithm is proposed to detect a hole quickly and easily. And the hole can be identified only by one time calculation. Second, a concise representation of the hole is proposed. A hole is recorded as a segment. Third, an approach to let a subset of the nodes located on the hole's boundary announce the hole information to the nodes in the vicinity was developed. Thetrade-off between the cost of hole information announcement and the benefit for future routing was discussed. Simulations show that compared with GPSR, HDAR reduces the length of routing path by 12.4% and the number of forwarding hops by 13.2% for all the paths in tested areas. And the length of long detour paths around the hole can be reduced by 61.2%. The number of hops can be reduced by 64.6% compared with GPSR. The simulation also indicates that the overheads of HDAR are only 16.6% those of HAGR. (F. Yan et. al ,2011) used the concepts of Rips complex and Cech complex to discover coverage holes and classify coverage holes to be triangular and non-triangular. This is based on topological approach. A distributed algorithm with only connectivity information was proposed for non-triangular holes detection. Some hole boundary nodes are found first and some of them initiate the process to detect coverage holes. Simulation results show that the area percentage of triangular holes is always below 0.1% when the ratio between communication radius and sensing radius of a sensor is two. It was also shown that proposed algorithm can discover most non-triangular coverage holes. (S. Fekete et al, 2004) proposed a boundary detection algorithm for sensors (uniformly) randomly deployed inside a geometric region. Proposed work is based on Statistical approach. The main idea is that nodes on the boundaries have much lower average degrees than nodes in the interior of the network. Statistical

arguments yield an appropriate degree threshold to differentiate boundary nodes. They consider a crucial aspect of self-organization of a sensor network consisting of a large set of simple sensor nodes with no location hardware and only very limited communication range. After having been distributed randomly in a given two-dimensional region, the nodes are required to develop a sense for the environment, based on a limited amount of local communication. They describe algorithmic approaches for determining the structure of boundary nodes of the region, and the topology of the region. Methods for determining the outside boundary, the distance to the closest boundary for each point, the Voronoi diagram of the different boundaries, and the geometric thickness of the network were also developed (R. Ghrist et al, 2005) proposed an algorithm that detects holes via homology with no knowledge of sensor locations; however, the algorithm is centralized, with assumptions that both the sensing range and communication range are disks with radii carefully tuned.This algorithm is based on Centralised approach based on Computational model. It uses only available connectivity information to detect single level coverage holes. Time complexity is O (n5), with n being the no of nodes. Approach gives no guarantee to detect hole boundary accurately. The methods presented are novel and of potentially great use in sensor networks. The use of topological methods allows one to dispense with assumptions about coordinates, distances, and orientations: this is a boon.

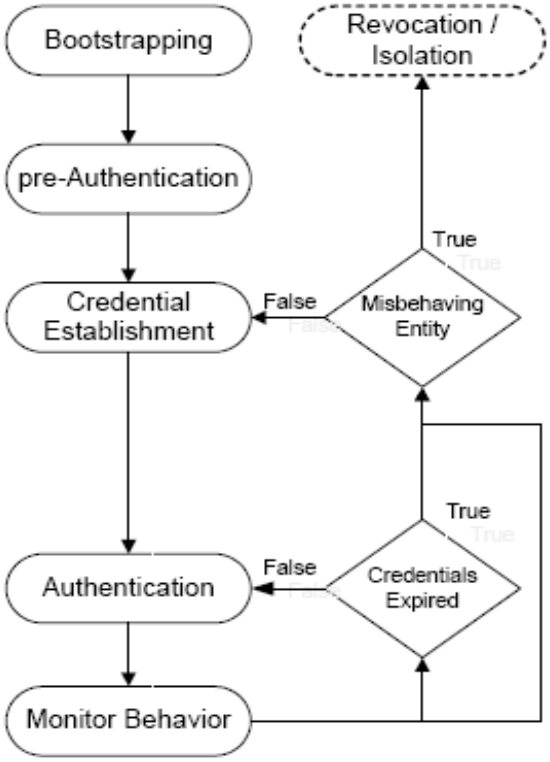
Ordered System:

A Leader Based Intrusion Detection System was proposed to detect and prevent malicious activities in Wireless Sensor Networks. A Leader was elected statically in the network for a group of nodes and it monitors those nodes comes under their control. Whenever a node gets activated it informs its status to the leader, so the leader knows about all the nodes information. But the entire new node should be informed about the leader and it takes time. To solve this kind of issues Dynamic Random Password Generation and Compression (DRPGAC) is proposed in this System.

Authentication Protocols:

Presented a new taxonomy for the classification of authentication protocols in ad hoc networks. Ad hoc networks can be classified into static and mobile networks. Sensor networks (SensNets) typically are static ad hoc networks. On the other hand, mobile ad hoc networks (MANETs) are autonomous systems of mobile nodes that are free to move at will. A hybrid network may also exist.From a security standpoint, ad hoc networks face a number of challenges. Attacks may come from anywhere and from all directions. Additionally, the lack of a clear line of defence and traffic concentration points poses a challenge to deploying security solutions in ad hoc networks. The broadcast nature of the transmission medium and the dynamically changing topology add even more complications. Furthermore, the reliance on node collaboration as a key factor of network connectivity presents another obstacle. In order to provide network security, support for authentication, confidentiality, integrity, non-repudiation, and access control should be provided. The authors believe that authentication is the cornerstone service, since other services depend on the authentication of communication entities. Authentication supports privacy protection by ensuring that entities verify and validate one another before disclosing any secret information. In addition, it supports confidentiality and access control, by allowing access to services and infrastructure to authorized entities only, while denying unauthorized entities access to sensitive data. In this paper the authors presents taxonomy for the classification of authentication protocols in ad hoc networks. They identify three major criteria for classification, based on a node's role in the authentication process, the type of credentials used for authentication, and the phase during which the establishment of credentials takes place.

Components of the Authentication Process:



Authentication is a process that involves an authenticator communicating with a supplicant using an authentication protocol to verify credentials presented by the supplicant in order to determine the supplicant's access privileges. A Trusted Third Party (TTP) may be involved as part of the authentication protocol. A generic authentication process has six major phases as shown in figure 1. Bootstrapping is the first phase, where a supplicant is securely provided, either offline or online, with something that it should have (a key) or something that it should know (a password) that authenticators would trust as a proof of the supplicant's eligibility to access protected resources or offer service.

Once the bootstrapping phase is completed, the supplicant is ready to participate in the network. The pre-authentication process is where a supplicant presents its credentials to an authenticator in an attempt to prove its eligibility to access protected resources or offer services.

Once the supplicant's credentials are verified, a credential establishment process is invoked to establish the supplicant's new credentials, which it will use as a proof of its identity and as a verification of its authorized state thereafter.

Upon success of all of the steps above, a supplicant is considered authenticated, which means that it is authorized to access resources protected by the authenticator. Within the authentication state, all communication between the supplicant and the authenticator is authenticated by the source and validated at the destination using the established credentials. While authenticated, a supplicant's behavior is monitored for fear of its being compromised or misbehaving. A compromised supplicant may get its credentials revoked (as in [10]) or its re-establishment of credentials request denied when its credentials expire. In both cases, the supplicant is isolated from the network.

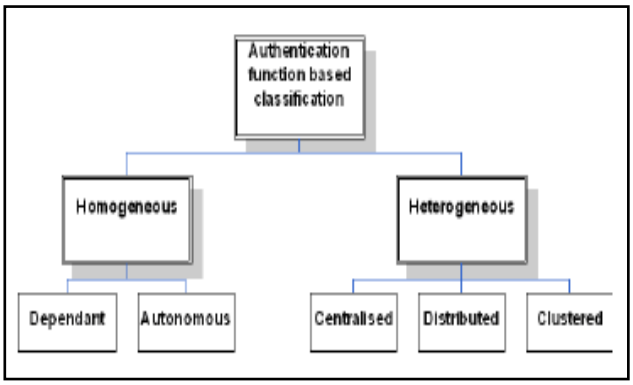
Functions in a Generic Authentication Process in Ad hoc Networks

Classification Based on Authentication Function:

Homogeneous Security Systems: Homogeneity indicates that all nodes in the network have the same role with respect to the authentication operation. This class of authentication protocols assumes that nodes in the network either make authentication decisions autonomously or they depend on information contributed by other nodes in the network to make such decisions. In general, trust based mechanisms fall under the homogeneous class of authentication protocols. Under the dependent homogeneous class of authentication protocols, authenticators rely on information from their trusted peers to make authentication decisions. On the other hand, in the autonomous homogeneous class, authenticators make authentication decisions autonomously without relying on their peers or any overlaying infrastructure

Heterogeneous : The heterogeneous class of protocols indicates that nodes in the network have different roles with respect to the authentication operation. This suggests that there is an underlying service in the network that is meant to aid other nodes in making authentication decisions (e.g., a trusted third party). Authentication protocols that are based on PKI or symmetric key fall under the heterogeneous authentication class.

The underlying service could be centralized, where one specialized node is responsible for providing that service, distributed, where service nodes are deployed anywhere in the network responding to service requests from any node, or clustered, where

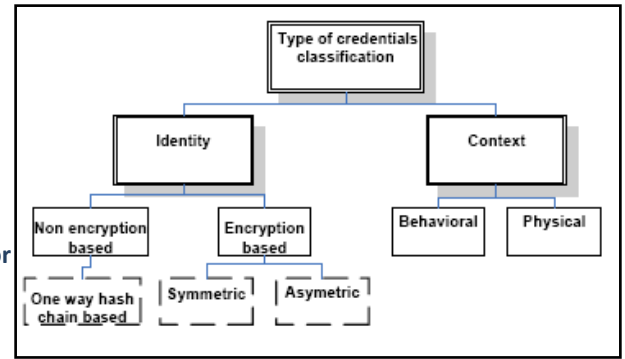


nodes are clustered and each cluster has a unique provider of the authentication service.

Classification Based on type of Credentials:

Identity-based credentials:

This category recognizes a unique possession owned by the supplicant that could be used to identify it with high confidence. Usually, this is in



the form of a key that is known to be unique to the supplicant. Identity based credentials can be further classified into encryption based and non-encryption based. An encryption based identity credential is a piece of information produced and

cryptographically signed using the key possessed by the supplicant in order to verify its possession of the key, and hence prove its identity. One form of non-encryption based identity credential is information that is hashed using a one-way key-based hash function and the key possessed by the supplicant. In order to verify the supplicant's identity, the authenticator must possess the same key (symmetric key) and the hashed information as the supplicant in order to re-generate the hash value and verify the claimed identity of the supplicant

Context Based Credentials:

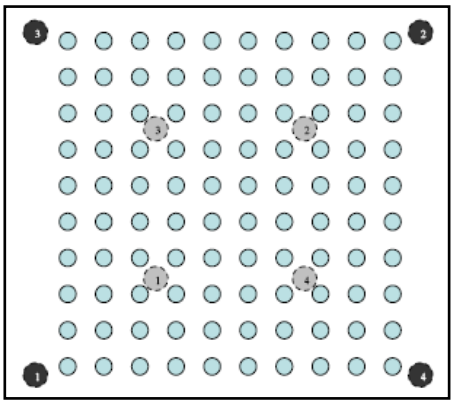
This category recognizes a unique contextual attribute of the supplicant that can be used to identify it with high confidence. Contextual based credentials can be behavioral or physical. Behavioral-based contextual credentials attempt to identify and authenticate a supplicant based on its pattern of behavior. On the other hand, physical characteristics based contextual credentials attempt to identify and authenticate a supplicant based on a physical characteristic that uniquely identifies it, such as its GPS location, RSSI (Received Signal Strength Indication), or SNR (Signal to Noise Ratio).

Classification Based on Establishment of Credentials:

The first category of authentication protocols under this classification assumes a pre-distribution offline phase (before deployment) where credentials are established. The second category of authentication protocols assumes that credentials are established post-deployment, such as protocols that rely on contextual information. The third category, like the first one, assumes pre-distribution of initial credentials. However, the actual credentials used for authentication are derived from the initial credentials post deployment.

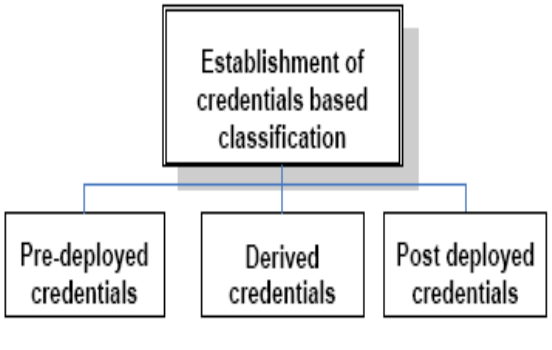
Classification based on establishment of credentials

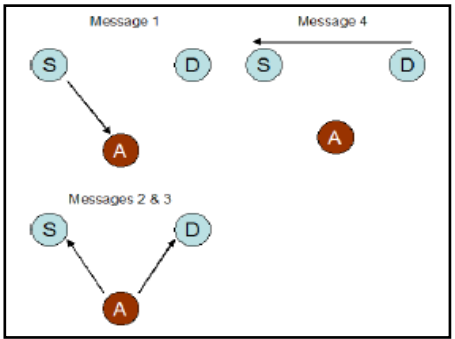
The authors have presented a generic authentication process and developed taxonomy of authentication protocols. They have also shown in this paper, through simulations, such as the counterintuitive increase in delay as the number of authentication severs increases for a high number of flows,



indicate that an authentication model needs. The

authors' work focuses on developing a formal model for reasoning about the properties of authentication protocols, a unified framework for the quantitative analysis of authentication protocols, and a generic architecture for authentication management.





Testing Methodology:

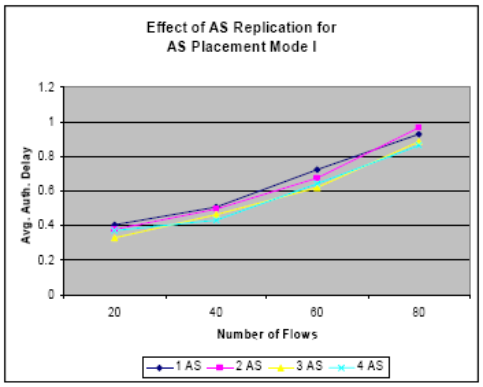
Authentication Protocols

In this paper the authors have justified the authentication management with a demonstrative simulation for a flat authentic server deployment model. In figure 15, they have shown a topology that we use to study the effect of these factors on the performance of the authentication operation. The network is a 10X10 grid of nodes in 500x500 topography. To study the effect of load over the network, they randomly generate sets of 20, 40, 60, 80, 100, 150, and 200 UDP flow. Before a flow starts, the source and destination nodes should authenticate one another through an authentication server as shown. Moreover, to study the effect of increasing the number of deployed servers, the author deployed 1, 2, 3, and 4 authentication servers. Furthermore, to study the effect of placement of authentication servers, they experimented with two placement models. The first model places authentication servers in the middle of quadrants as shown. The second model places servers at the edges of the network as seen in figure 15. Finally, they compare the flat deployment model used in the above simulations to a hierarchical deployment model, where the authentication status of each node is known to single authentication server.

Grid Topology. (First authentication server placement model is shown in gray. Second AS placement model is shown in black.)

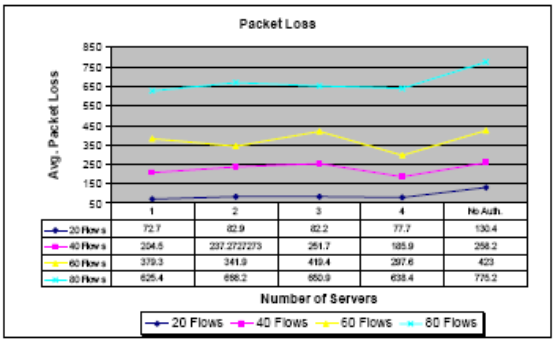
Flat Authentication Model. "S" denotes a source node, "D" denotes a destination node, and "A" denotes an authentication server.

The performance of the authentication operation is measured in terms of the delay caused by node authentication, while that of the network is measured in terms of packet loss. The simulation results indicate that the authentication delay increases as the load over the network increases. The results are consistent for both placement models and regardless of the number of authentication servers deployed.



Simulation results showing authentication delay as the number of flows increases from 20-80 flows for 1-4 authentication servers placed using model I. Delay of each set of flows is averaged over 10 simulation runs

While it is expected that the network performance decreases as the authors introduce the authentication operation into the network, the simulation results show that the packet loss decreases when authentication of nodes is mandated before a flow starts. This is due to the "backoff" effect of authentication (source and destination of flows are authenticated before flows are allowed in the network). Therefore, the overhead added by authentication may be offset by the benefit of backoff. Figure 19 compares packet loss when authentication is mandated before a flow starts versus when no authentication is required.



Contribution Work done by various Researchers in the field of coverage hole detection and healing is studied in Section I describes the characteristics of various proposed coverage hole detection and healing algorithm. A modified hole detection and healing method is proposed, that could remove the drawbacks of existing algorithms. Proposed method is a distributed and localized algorithm that operates in two distinct phases. First, is Distributed Hole Detection (DHD) proposed to identify the boundary nodes and discover holes. Second, is hole healing which uses a virtual forces based hole healing algorithm. Unlike existing algorithms, proposed algorithm uses QURD based node detection method and could be cost efficient as node selection depends upon the lowest residual energy node. QUAD Rule, ensure that each individual node is capable of communicating in 3600 with respect to its communication range. The QUAD rule specifies that a node is not a stuck node if where there exists at least one 1-hop neighbour within the range of angle spanned by itself which is less than $\pi/4$.The process of discovering a hole is first initiated by the identification of stuck nodes. Each node executes the QUAD rule to check whether the node itself is a stuck node or not. Thus providing energy efficient and cost efficient Hole detection and Healing method.

Proposed System:

Dynamic Random Password Generation and Comparison (DRPGAC) technique is proposed, it has three modules such as Node identification, Mutual Authentication and Secret Key updating. The overall functionality of DRPGAC is depicted clearly the assumptions are made for the DRPGAC approach where the network G is a wireless network. The node may be of any type [laptop, mobile, PC etc.] which can communicate using wireless communication medium. Base station BS is the responsible administrator for the entire network can assign ID, key, key verification etc, in the network.

Modules:

1. Node identification
2. Mutual Authentication
3. Secret Key updating

Algorithm:

Algorithms can be expressed in many kinds of notation, including natural languages, pseudo code, flowcharts, darken, programming languages or control tables (processed by interpreters). Natural language expressions of algorithms tend to be verbose and ambiguous, and are rarely used for complex or technical algorithms. Pseudo code, flowcharts, drakon charts and control tables are structured ways to express algorithms that avoid many of the ambiguities common in natural language statements. Programming languages are primarily intended for expressing algorithms in a form that can be executed by a computer, but are often used as a way to define or document algorithms.

Dynamic Random Password Generation and Comparison technique is used for Node

Identification. A dynamic number is generated using Key GEN method where the IMEI number is added and appends at last with the node-ID.

Key Generation

For I =1 to N

V i = substring (Node-ID, 4);

Key i = append (IMEI I, Vi + IMEI I);

For i =1 to length (Key i)

IMEI I = IMEII mod 2;

END I

Here Key is generated for each node and save in Database, key is generated by node id is append to random number and mod with 2 then key generated and save in Database.

Sending Data from Source to Destination:

For I =S to D

If (Node i ==D) then stop

Else

If (Node i.ID, Node i. Key. Exists (BS-DB. record))

Node i+1 .data=Node i. data

Else

Next I

Example for key generation

Step 1: V1 = Substring (TALTA0001, 4)

= TALTA

Step 2: IMEI 1= 278373612(randomly generated)

= IMEI 1 mod 2

Step 3: IMEI 1 = 010111010

Step 4: key 1 = Append (IMEI 1, V1+IMEI 1)

= 010111010TALTA010111010

Conclusions:

In this paper, a broad survey of a vital problem in sensor networks that are the detection of holes and healing process in network is focused. Coverage holes are the most important to detect as they play a vital role in assuring good Quality of Service. Identification of various coverage hole detection algorithm is therefore important. The work done by various authors in a sensor network is described in details. A literature review of holes in WSN is provided. To remove the drawbacks of existing method, a modified hole detection and healing method is proposed, that could remove the drawbacks of existing algorithms. HEAL is a distributed and localized algorithm that operates in two distinct phases. First, is Distributed Hole Detection (DHD) proposed to identify the boundary nodes and discover holes. Second, is hole healing which uses a virtual forces based hole healing algorithm. Unlike existing algorithms, proposed algorithm uses QURD based node detection method and could be cost efficient as node selection depends upon the lowest residual energy node. Thus providing energy efficient and cost efficient Hole detection and Healing method.

References:

Yun Wang, Weihuang Fu, and Dharma P. Agrawal, Life Fellow, “Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks” IEEE TRANSACTIONS ON

PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 2, FEBRUARY 2013

Alexander G. Tartakovsky, Aleksey S. Polunchenko, and GrigorySokolov, "Efficient Computer Network Anomaly Detection by Changepoint Detection Methods" IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, VOL. 7, NO. 1, FEBRUARY 2013

J. Yang and Z. Fei, HDAR: Hole Detection and Adaptive Geographic Routing for Ad Hoc Networks, 2010 Proc. 19th Int. Conf. Comput. Commun. Networks, pp. 1–6, Aug. 2010. Wei-Cheng Chu and Kuo-Feng Ssu (2014), Location free boundary recognition in mobile wireless sensor networks with a distributed approach, Science Direct Computer Networks, 70, 96-112.

F. Yan, P. Martins, and L. Decreusefond (2011), ConnectivityBased Distributed Coverage Hole Detection in Wireless Sensor Networks, IEEE Glob. Telecommun. Conf. - GLOBECOM, 1–6. Dezun Dong, Yunhao Liu and Xiangke Liao (2009), FineGrained Boundary Recognition in Wireless Ad Hoc and Sensor Networks By Topological Methods

MobiHoc. S. Fekete., A. Kroller and D. Pfisterer, S. Fischer and C. Buschmann (2004),Neighborhood-based topology recognition in sensor networks Algorithmic Aspects of Wireless Sensor Networks(ALGOSENSORS) Springer LCN, 3121, 123–136.

R. Ghrist, and Muhammad (2005)A Coverage and HoleDetection in Sensor Networks via Homology, Proceedings of IPSN', 254-260.

P. Corke , R. Peterson and D. Rus (2007) , Finding Holes in Sensor Networks, IEEE Workshop on Omniscient Space: Robot Control Architecture Geared toward Adapting to Dynamic Environments,

ICRA. Y. Wang, J. Gao, and S.B. Mitchell (2006), Boundary recognition in sensor networks by topological methods, MobiCom ACM 122-133.

S. Kroller, P. Fekete, D. Pfisterer, and S. Fischer (2006), Deterministic Boundary Recognition and Topology Extraction for Large Sensor Networks, ACM-SIAM Symposium on Discrete Algorithms, 1000–1009.

M. R. Senouci, A. Mellouk, S. Member, and K. Assnoune (2013), Localized Movement-Assisted Sensor Deployment Algorithm for Hole Detection and Healing, IEEE transactions on parallel and distributed systems , 1–11.

Xiaoyun. Li and D. K. Hunter (2008), Distributed Coordinatefree Hole Recovery, 189–194. G. Wang, G. Cao, and T. L. Porta (2003), A bidding protocol for deploying mobile sensors, 11th IEEE International Conference on Network Protocol ICNP , 315.324.

S. Babaie and S. S. Pirahesh (2012), Hole Detection for Increasing Coverage in Wireless Sensor Network Using Triangular Structure, IJCSI 2, 213–218. G uiling Wang, Guohong Cao, and Tom La Porta (2004), Movement-assisted sensor deployment, In IEEE INFOCOM. 4,12-18.