ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 7; Page No. 68-73

Analysis on Wireless Sensor Networks & Emergence of Three tier Information Intruder Cache

M. Venkateswara Rao[1] Ch. Sangeetha[1],

[1] Associate Professor at Vignana Bharathi Institute of Technology

[2] Research Scholar, Computer Science Engineering at Vignana Bharathi Institute of Technology

ABSTRACT

This paper describes the concept of sensor networks an intruder compromised node in one place can be relocated or duplicated to other places to continue attacks hence detection and isolation of the intruder may have to be conducted repeatedly wasting scarce network resources. Detecting intruder sensor whose content have been crucial in the settings as the attacker can reprogram the sensor to act on his behalf, verifying content is difficult as physical access to the sensors is often infeasible. Before intruder detection just identified the compromised node using algorithms in two tier our proposed framework three tier consisting of a verifiable intruder reporting scheme, a quorum based caching schemefor efficiently propagating intruder reports to the whole network,and a collaborative Bloom Filter scheme for handlingintruder information locally. System identifies the attacker in the network prevents to send the data to receiver and also avoids the data when the intruder is attacked in the sensor network at that time it uses other routing path to reach the destination.

Keywords: Wireless Sensor Networks, Intruders Information cache, Collaborative Bloom Filter, Attacker.

INTRODUCTION:

Purpose of laptops cell phones PDAs GPS devices EFID and intelligent electronics in the post PC computing devices has become cheaper more mobile distributed and pervasive in daily life. Possible to construct from commercial off-the –shelf components a wallet size embedded system with the equivalent capability of a 90's PC, supports with scaled down windows or Linux operating systems. The emergence of wireless sensor networks is essentially the latest trend miniaturization and ubiquity of computing devices. Wireless sensor node consists of sensing computing communication actuation and power components are integrated on a single or multiple boards packaged in a few cubic inches.In general users can retrieve information of interest from wireless sensor node by injecting queries and gathering results from the base stations which behave as an interface between users and the network considered as a distributed database. Sensor networks will ultimately be connected to the internet through global information sharing becomes feasible.

Wireless sensor network is highly anticipated in the identified by Business week as one of the most important technology for the 21st century.

Wireless sensor networks consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions such as temperature sound vibration pressure motion or pollutants for wireless sensor networks including monitoring tracking, system simulator included in this add-on allows the modelling of arbitrary wireless sensor network topologies in rural urban indoor tunnels.

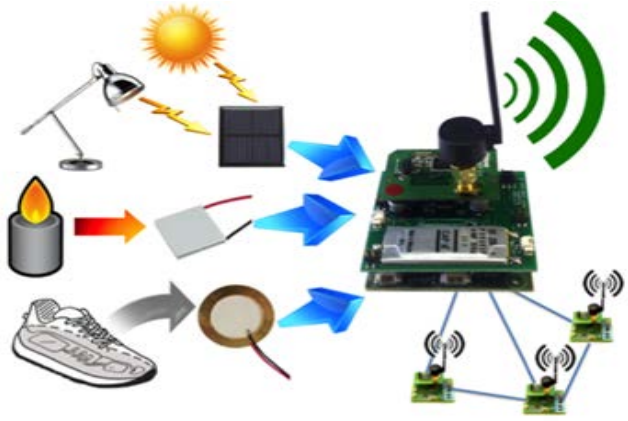

Figure 1 Power Platform of Wireless Sensor Networks

Wireless sensor networks have garnered significant attention consist of set of spatially distributed autonomous devices usually battery-powered and designed to operate for a long period of time consequently minimizing the energy consumption design and very efficient wireless transmission schemes together with ultra-power platforms. The radio in both transmit and receive modes consumes the bulk of the total power consumption of wireless sensor networks systems therefore protocol optimization is one of the main sources of significant energy reduction to be able to achieve self-powered autonomous systems. Power optimized hardware and software framework for wireless designed to handles sensor networks and related applications innovating features of the platform energy efficient MAC protocol much more light memory usage for acceleration of part of the software stack.

SECTION II

2. Related Work:

Sensor node consists of a great number of nodes of the same type sensor nodes, which are spatially distributed and cooperate with each other. Each such node has a sensing element sensor, a microprocessor microcontroller, which process sensor signals, a transceiver and an energy source. Distributed over the object, sensor nodes with the necessary sensors make it possible to gather information about the object and control processes which take place on this object. Wireless sensor networks offer unique opportunities for monitoring and data collecting from a number of spatially distributed sensor nodes. In addition to providing distributed sensing of one or a few parameters of a big object like a building or open space for example, wireless sensor network may be installed in a building for automatic control of load-bearing constructions' conditions engineers determine the places on the building most appropriate for data measuring. In these places autonomous sensor nodes with necessary sensing elements are installed. After installation they start to interact and exchange data. Receiving these data from the sensor nodes and comparing measurement data from each of the sensor node with its position, building structure specialists can in real time mode supervise, control and predict emergency situations.

The interest is caused by the fact that wireless sensor network applications are highly promising and help to solve a wide range of problems which are to be described below. Also, technological progress in the microelectronics made it possible to produce rather small, productive, energy effective and cheap sensor nodes, and it allows introducing and using advantages of wireless sensor network technology everywhere and right now.

Wireless sensor network technologies started to actively develop in mid 1990s, and in the beginning of 2000s the microelectronics development made it possible to product rather inexpensive elementary base for sensor nodes. It also became possible due to the rapid development of wireless technologies and microelectromechanical systems. Constant wireless devices price decreasing, their operating parameters improving make it possible to gradually migrate from using wireline technologies in telemetric data collecting systems, remote diagnostics techniques, data exchange. A lot of branches and market segments production, constructing, different types of transport, life support, security, warfare are interested in wireless sensor networks deployment, and their number is permanently increasing. It is caused by technological processes complication, production development, increased needs in security field and resources use control. In emergency management, sensor nodes can sense and detect the environment to forecast disasters before they occur. In biomedical applications, surgical implants of sensors can help monitor a patient's health. For seismic sensing, ad hoc deployment of sensors in volcanic areas can detect occurrence of earthquakes and eruptions. With the development of semiconductor technology there are new wireless sensor network practical applications appearing in industry, household and also in military field. The usage of inexpensive wireless sensor devices for remote monitoring opens up new fields for telemetry and control systems applications, such as:

Military target tracking and surveillance

Timely detecting of possible mechanism failure, when controlling such parameters as vibration, temperature, pressure, etc.

Control of access to remote monitoring object

systems in real time mode.
Buildings and constructions condition control automation.
Smart house.
Energy saving and resource saving.
Biomedical health monitoring.
Ecological parameters of environment control.
Natural disaster relief.
Hazardous environment exploration and seismic sensing.

SECTION III

3. Problem Definition: Distributed autonomous sensors such as temperature sound pressure pass their data through the network to main location are bi-directional enabling control of sensor activity. Wireless sensor network built of nodes few hundred or even thousands where each node is connected to sensor as typically several parts a radio transceiver with an internal antenna or connection to a microcontroller for interfacing with the sensor and an energy source. Communication between source to destination might have intruder, protect our packet information our proposed analysis provides the three tier architecture. A sensor node, such as restricted processing capabilities and a limited amount of energy, have an impact on all the parameters of a WSN. Taking into account the energy characteristics of transmitters in sensor nodes and their high susceptibility to interference, the quality of communication between sensor nodes can vary significantly with time.

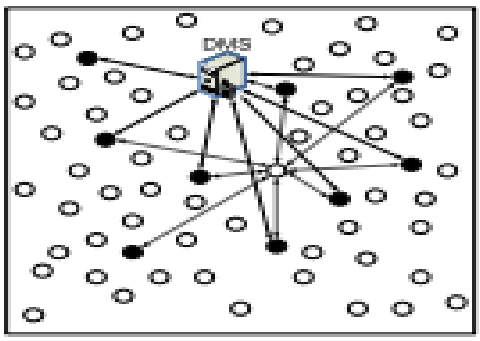

Figure 1 Proposed Problem Definition

We have many intruder detection techniques our proposed framework is three tier for wireless sensor networks which provides the first tier intruder disseminates aggregates to network due to critical role the dedicated membership server may become an attractive target of attacks. Dedicated membership server may locate directly or block the communication between the dedicated membership or the remaining networks. Protection makes it hard for the adversary to trace attack or isolate the dedicated membership server. Middle tier isan intruder information caches picks the sensor nodes from sensor network, intruder information cached removed or modified, verifying intruder information to prevent fabricating and duplicating intruder information to maintain high availability of the information. Third tier collaboratively identify intruders and report intruder information. Sensor nodes maintain own intruder information based on the periodical updates disseminated by the dedicated membership server and determines the legitimacy of sensor nodes query intruder information cache to obtain latest intruder information when necessary.

3.1. Dijkstra's algorithm

For a given source vertex (node) in the graph, the algorithm finds the path with lowest cost (i.e. the shortest path) between that vertex and every other vertex [11]. It can also be used for finding costs of shortest paths from a single vertex to a single destination vertex by stopping the algorithm once the shortest path to the destination vertex has been determined.

Algorithm

The node at which we are starting is called the initial node. Dijkstra's algorithm will assign some initial distance values.

1. Assign to every node a distance value: set it to zero for our initial node and to infinity for all other nodes.

2. Mark all nodes as unvisited. Set initial node as current.

3. For current node, consider all its unvisited neighbors and calculate their *tentative* distance (from the initial node). For example, if current node (A) has distance of 6, and an edge connecting it with another node (B) is 2, the distance to B through A will be 6+2=8. If this distance is less than the previously recorded distance (infinity in the beginning, zero for the initial node), overwrite the distance.

4. When we are done considering all neighbors of the current node, mark it as visited. A visited node will not be checked ever again; its distance recorded now is final and minimal.

5. If all nodes have been visited, finish. Otherwise, set the unvisited node with the smallest distance (from the initial node, considering all nodes in graph) as the next "current node" and continue from step 3.

SECTION IV

4.1. Verifiable Intruder Reporting (VIR): Intruder reports [5] generated by a single node are not trustable since the reporting node itself could have been compromised. Therefore, detectors should collaborate to identify intruders, and identification conclusions should be made based on the agreement among the majority of the detectors. After that, intruder information should be known to non-detecting nodes. Hence, we propose a verifiable intruder reporting (VIR) scheme, which works as follows:

(i) When a node is deployed or relocated to a place, it authenticates with every 1-hop neighbor and disseminates shares of its private key to these neighbors.

(ii) If this node is identified as an intruder by the majority of its 1-hop neighbors, these neighbors can collaboratively derive the private key, which can be used as the intruder report.

(iii) Intruder reports can be verified by every node based on a small amount of secrets preloaded to these nodes.

In this way, verification of intruder reports is easy and decentralized (no need for online trusted membership managers), and the cost for transferring reports is low.

The VIR scheme is designed based on a combination of the secret sharing the Elliptic Curve Cryptography and the Merkle hash tree techniques:

Detailed Description

1) System Initialization: Let *E/Fp*be an elliptic curve $y2 = x3 + ax + b$ over a finite field *Fp*, *G* be a *q*-order group of points of *E/Fp*, and *H* be a hash function mapping an arbitrary string to a point in *G* .The DMS has a private key[10] $K_S^-$and a public key $K_S^+ = K_S^- H(s)$.

Before each sensor node (with ID *u*) is deployed, it is preloaded with the following information: [5]

1) $H(u)$: the hash of *u*. This is computed offline in order to reduce computation overhead at sensor nodes.
2) $K_S^+ = K_S^- H(s)$, the public key of DMS.
3) $K^+_u = K^-_u H(u)$, the public key of sensor node *u*.
4) Hash tree auxiliary values for authentication of K^- the auxiliary values can be used to verify the validity of K^-_u .
5) $cert_u = \{u, K+ u , \hat{}pu, i(i = 0, \cdots, m)\}_{K-s}$

After the sensor network is deployed, assuming the network is secure for a short time, each node obtains the actual IDs and locations of all other nodes within its 2-hop neighborhood.

Then, each node broadcasts its public key and hash tree auxiliary values to its 1-hop neighbors. In addition, each node (denoted as *u*, where *u* is its ID), arbitrarily constructs a $t = \_n/2\_$ (the number of its 1-hop neighbors is *n*) degree polynomial (over finite field *Fp*) denoted a $fu(x) = a0 + a1x + \cdots + atxt$, where $a0 = K-u$, and sends to each 1-hop neighbor *vi* a share $fu(vi)$ [5].

4.2. Collaborative Bloom Filter: The DMS periodically disseminates reports of intruders identified since the last dissemination, and this information should be recorded by each sensor node. However, as time elapses, the number of intruders increases and recording these intruders may consume a large portion of sensor nodes' storage, which is undesirable since the primary function of a sensor node is sensing and processing data and security schemes should occupy as little resource as possible. To address this issue, I propose a collaborative Bloom Filter (CBF) scheme in this section.

To test the legitimacy of a newly deployed or relocated node v, the testing node first searches its own Bloom Filter for v. If v is not found, it is immediately considered as good. Otherwise, neighbors of the testing node are invited to collaboratively test v. Specifically, the testing node broadcasts a query message to its neighbors, each neighbor searches its own Bloom Filter for v, and sends back the result to the testing node. Having received all replies from neighbors, the testing node counts the number of neighbors claiming v as good. If and only if the number is greater than a certain threshold (denoted as γ), v is considered as good.

False Positive Probability and False Negative Probability [5]:

• *p*: false positive probability when using a single Bloom Filter

• *q*: probability that a neighbor is innocent (good)

• *x*: number of neighbors replying "the tested node is good"

• *y*: number of neighbors replying "the tested node is bad"

• *p*(*TG*): probability that the tested node is actually good

• *p*(*TB*): probability that the tested node is actually bad

• *p*(*CG*|*TB*) (false negative probability): probability that the tested node is considered good if it is actually bad

• *p*(*CB*|*TG*) (false positive probability): probability that the tested node is considered bad if it is actually good

When a neighbor of a testing node receives a query for collaborative testing, its response is determined by two factors: whether the neighbor itself is innocent (good) or compromised (bad), and the false positive probability when using its own Bloom Filter. Naturally we assume that a good neighbor cooperates and reports the exact result of searching its own Bloom Filter, but the result reported by a bad neighbor is reverse to the exact result of searching.

SECTION V

5. Comparative Study:

Wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. A sensor network consists of multiple detection stations called sensor nodes each of which is lightweight and portable equipped with a transducer microcomputer transceiver. The transducer generates electrical signals based on sensed physical effects, microcomputer processes and stores the sensor output and transceiver receives commands from central computer and transmits data to that computer. A sensor network is composed of a network controller and a large number of densely deployed resource constrained sensor nodes, controller connects to the network every time at an arbitrary position with static topology. Communication require to transfer data transducer to receiver trust be compromised sensor nodes are innocent before they are deployed at a certain rate. Existing intruder schemes are run by sensor nodes misbehavior of compromised nodes can be detected by its neighbors and the identified intruders can be isolated compare to earlier system our proposed work interaction with entities, sensor nodes generates intruder reports that can be verified by other node and send them to a certain set of intruder information caches every time to intruder collect the report for intruders that have been identified the previous query and then disseminates the IDs of these intruders to all sensor nodes in a secure receiving every sensor node records these intruders if the sensor node is also an information intruder removes the intruders from its cache. When a node connects a neighborhood can use their own knowledge about identified intruder to determine if the new arrival is intruder.

Conclusion

This paper presents a three tier framework for intruder information sharing sensor networks identifies the attacker prevents to send the data, before intruder detection system just identifies the attack then classifies the data into abnormal and normal data. Our proposed three tier scheme for system wide propagation of intruder information and collaborative bloom filter for local management of intruder information and also choose other routing path if an intruder finds in the one of routing path efficiently.

Reference

1. Hui Song, Sencun Zhu, Wensheng Zhang, Guohong Cao: Least privilege and privilege deprivation: Toward tolerating mobile sink compromises in wireless sensor networks. TOSN 4(4): (2008).
2. Chanjun Yang, Jianming Zhou, Wensheng Zhang, Johnny Wong: Pairwise key establishment for large-scale sensor networks: from identifier-based to location-based. Infoscale2006: 27
3. B. Parno, A. Perrig and V. Gligor, "Distributed detection of nodereplication attacks in sensor networks," *IEEE S&P*, pp. 49–63, May2005.

4. Y. Yang, X. Wang, S. Zhu, and G. Cao, "Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks," *SRDS*, pp. 219–230, October 2007.

5. Nalin Subramanian, Chanjun Yang, Wensheng Zhang: Securing distributed data storage and retrieval in sensor networks. Pervasive and Mobile Computing 3(6): 659-676 (2007).

	**M. Venkateswara Rao** B.Tech IT from VNR Vignana Jyothi Institute of Engineering M.Tech CSE From JNTUH college of engineering Hyderabad.With eleven years of Academic experience currently he is Asso.Prof. at Vignana Bharathi Institute Of Technology, guided many UG & PG students. His research areas include Data Mining, Security Issues, Networking, Cloud Computing.
	**Ch. Sangeetha** pursuing M.Tech Computer Science Engineering from Vignana Bharathi Institute of Technology B.Tech Information Technology from Sridevi Women's Engineering College. Her interested research areas include Data mining, Networks, currently focusing on Wireless Sensor Networks.