Interlock Triple Authentication and Data Routing Protocol in WSN

EDWIN RAJESH.A*, DR.PONMUTHURAMALINGAM.P**

*(Asst.Professor,Dept.of Comp.Science,Bishop Appasamy College,Coimbatore-641018

** (RJD for Collegiate Education, Coimbatore-641018)

ABSTRACT

To built up sensor clusters is an effective way to improve scalability and longevity of wireless sensor network (WSN).Nevertheless, security is a challenging issue in cluster-based WSNs, since sensors are usually deployed in unattended environments. Additionally, limited memory, processing power, and communication range of sensor nodes (SNs) make traditional cryptographic schemes infeasible. In addition, cluster heads (CHs) are usually responsible for data aggregation and consume more energy than the member nodes, which cause early termination from energy exhaustion. Moreover, data decryption and encryption to ensure secure transmission demand more computation and hence shorten the network life.

To address these challenges, we introduce a method Interlock Triple Authentication to secure data transmission in WSN. This method has three layers and one DNA station. The three layers are Host discovery layer, TCP port scan layer and evaluation layer. The DNA station has base node, sensor node and service detection with the support of IP trace and IP test book. Base node is responsible for specification analysis and base node has event DNA.

Keywords: Wireless sensor networks, Security,Cluster heads, Attacks, Trust, Layers and DNA station.

1.INTRODUCTION

Wireless Sensor Networks are dynamic and may contain numerous kinds of device nodes. The surroundings are heterogeneous in terms of each hardware and computer code. In anticipating data to the base station, wireless sensor networks (WSNs) face some security challenges since such networks impose resource constraints that need to be addressed by the routing mechanism. This paper analyse, explores, and informs researchers regarding the landscape of multipath routing by providing the motivation behind multipath routing deployment. Finally, this paper analyzes the security requirements and common attacks in wireless sensor networks. We provide a classification of secure multipath routing protocols on the basis of nature of defence against the WSN attacks. According to the classification, we investigate the existing secure multipath routing protocols within the WSN domain by discussing their strengths, limitations, and efficiency analysis. A provisional study of the recommended classification is based upon the multipath technique, additional security infra-structure, security requirements, corresponding attacks, and efficiency in pursuit of effective secure routing in wireless sensor networks.
Therefore, various attacks can leads to many security problems.

RELATED WORDS

In first, technical challenges and style principles are introduced regarding hardware development, system architectures and protocols, and computer code development. The aim of this analysis work is to advance a mechanism that may observe and overcome the result of black hole attack in a sensor network. The paper proposes a lively detection routing of information for higher security and trust. The most goal of the scheme is to make sure that the nodal knowledge safely reaches the sink and aren't blocked by the black hole.

The demerit during this paper was it'll not find the sensor nodes as a black hole node. A detection route confirms to a route while not knowledge packets whose goal is to satisfy the individual to launch an attack that the system will realize the attack behaviour stick the black hole location.. During this approach, the supply node stochastically selects the associate adjacent node with that to get together, that the address of the adjacent node is employed as destination address to malicious nodes to send a reply message.

3. WIRELESS SENSOR NETWORK

The WSN is made of "nodes" – from many to many a whole bunch or perhaps thousands, wherever every node is connected to at least one (or generally several) sensors. The value of sensor nodes is equally variable, starting from any to many dollars, looking on the complexness of the individual sensor nodes. Size and value of the constraints in this sensor elements are a sensor node are lead to the corresponding constraints in the resources like as energy, memory, processor speed and the communications information measure. The topology of the WSNs will vary from an easy star network to a complicated multi-hop wireless mesh network. That the cross-layer may be accustomed build the optimum modulation to enhance the transmission performance, like rate, energy efficiency, QoS (Quality of Service), etc.
Sensor nodes may be imaginary as little computers that are extraordinarily basic in terms of their interfaces and their elements. They act as an entryway between sensor nodes and therefore the user as they usually forward knowledge from the WSN on to a server. Different special elements in the routing primarily based networks are routers, designed to compute, calculate and distribute the routing tables.

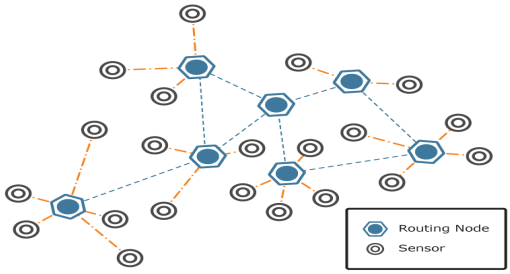


Figure 3.1: Sensor Network

Sensor node:
Although wireless sensor element nodes have existed for decades and used for applications as various different types of earthquake measurements to warfare, the trendy development of little sensor nodes dates back to the 1998 good dust project and therefore the NASA sensor Webs Project one among the objectives of the good dust project was to make autonomous sensing and communication among a metric capacity unit of space.

Sensor: Sensors live physical knowledge of the parameter to be monitored. The continual analog signal created by the sensors is digitized by an analog-digital converter and sent to controllers for the additional process. A sensing element node should be little size, consume extraordinarily low energy, operate in high volumetrical densities, be autonomous and operate unattended, and be adaptive to the surroundings.

Routing Node: Routing is that the method of choosing best methods in an exceedingly network. In the past, the term routing additionally meant forwarding network traffic among networks. However, that latter perform is best represented as forwarding. Routing is performed for several types of networks, as well as the telephone network (circuit switching), electronic knowledge networks (such because of the Internet), and transportation networks. This text thinks about primarily with routing in electronic knowledge networks exploitation packet switch technology.

4. EXISTING SYSTEM

Single-path routing may be an easy routing protocol, however, is well blocked by the attacker. Therefore, the foremost natural approach is via multi-path routing to the sink. Although there's an attack in some route, the information will still safely reach the sink. Multi-path routing protocols may be classified into two categories looking on whether or not the information packet is split. One is multi-path routing while not share division. The other is multi-path routing with share division, i.e., the packet is split into shares, and totally different| completely different shares reach the destination via different routes. Non-share-based multi-path routing. There are totally different multi-path route construction strategies. Another paper proposes a multi data flow topologies (MDT) approach to resisting the selective forwarding attacks within the MDT approach, the network is split into two data flow topologies.

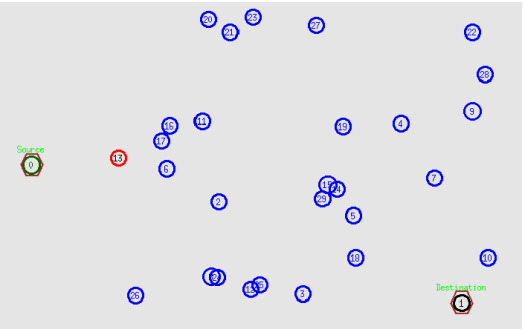


Figure 4.1: Drawbacks in the Existing

The basic plan of the unfold algorithm is to remodel a secret message into multiple shares, that is named a (T, M) threshold secret sharing scheme. The M shares are delivered by multiple freelance methods to the sink specified, although a little range of shares is born, the key message as an entire will still be recovered. The advantage of this algorithm is that through multi-path routing, every path routes just one share, and therefore the attacker should capture a minimum of T shares to revive nodal data, that will increase the attack issue.

Thus, the privacy and security may be improved and multi-path routing algorithms are deterministic specified the set of route methods is predefined below a similar topology. This weakness opens the door for numerous attacks if the routing algorithm is obtained by the individual. For the weakness mentioned higher than, proposed four random propagation strategies: random propagation (PRP), directed random propagation (DRP), non-repetitive random propagation (NRRP), and multicast tree assisted random propagation (MTRP).

In multi-to-one knowledge assortment WSNs, we tend to argue that for traditional "slicing and assembling" or multi-path routing 0techniques, sliced shares can merge within the same path with high chance, and this path may be simply attacked by black holes. so a Security- and Energy-efficient Disjoint Route (SEDR) scheme is planned to route sliced shares to the sink with randomised disjoint multipath routes by utilizing the obtainable surplus energy of sensor nodes. It additionally proposes a resilient trust model, Sensor Trust, for hierarchical WSNs. Introduces the conception of attribute similarity to find probably friendly nodes among strangers.

5.PROPOSED SYSTEM

This method has three layers and one DNA station. The three layers are Host discovery layer, TCP port scan layer and evaluation layer. The DNA station has base node, sensor node and service detection with the support of IP trace and IP test book. Base node is responsible for specification analysis and base node has event DNA.

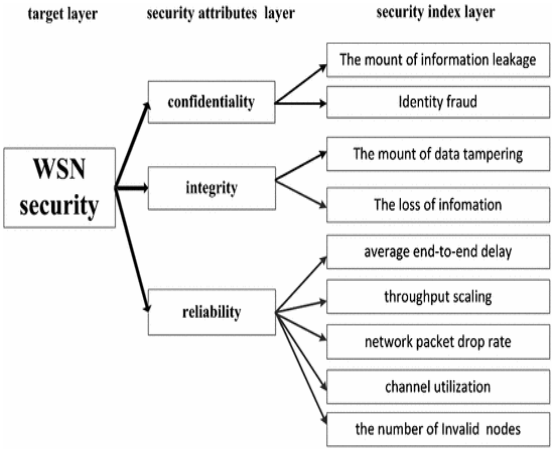


Figure: WSN Security Layer

I Host Discovery Layer

Host discovery layer is the first authentication layer that has three types of scanning methods. List scan, UDP ping and trace path to host.

List scan : is been degenerate form of host discovery that simply lists each host of the network(s) specified, without sending any packets to the target hosts. By existing, Nmap still does reverse-DNS resolution on the hosts to learn their names. It is useful information how hostnames giveout simple hostnames. For example, inf.ca is the name of one company's canada firewall. The total number of IP address is reported by Nmap at the end. The list scan is a clear check to ensure that you have proper IP addresses for your targets. If the hosts sport domain names you do not recognize, it is worth investigating further to prevent scanning the wrong network.

UDP ping: Host discovery in another method is the UDP ping, it sends a UDP packet to the given ports. For maximum ports, the packet will be empty, though the use of protocol-specific payload which brings out a response. And in the section called "UDP payloads: nmap-payloads" provides a descriptive database of payloads. Packet information's can also be affected with the --data-string --data, , and --data-length options.

The port list takes the specified method as with the previously discussed -PS and -PA options. If ports are not specified, the default port is 40125. This default can be constructed at compile-time by changing DEFAULT_UDP_PROBE_PORT_SPEC in nmap.h. A highly irrelative port is been used by default because sending to open ports is often not recommended for this particular scan type.

By reaching the closed port on the target machine, the UDP probe should evoke an ICMP port unreachable packet as result. This implied to Nmap that the machine is up and feasible. Many other types of ICMP errors, like host/network unreachable or TTL outstrips a indicative of a down or unreachable host. A inadquency of response is also interpreted on this process. If an open port is attained, most services are simply ignored the empty packet and fail to return any response. So the default probe port is 40125, which is highly absurd to be in use. A limited services, such as the Character Generator (charge) protocol, will respond to an empty UDP packet, and thus acknowledge to Nmap that the machine is available.

The main disadvantage of this scan type is that it sidestep firewalls and filters that only screen TCP. For example, I once owned a Linksys BEFW11S5 wireless broadband router. The external interface of this device filtered all TCP ports by default, but UDP probes would still obtain port unreachable messages and will give away the device.

Trace path to host : Trace routes are executed by post-scan using information from the scan results to regulate the port and protocol most likely to reach the target. It reinforce all scan types except connect scans (-sT) and idle scans (-sI). All traces use Nmap's dynamic timing model and are executed in parallel.

Traceroute performs by sending packets with a low TTL (time-to-live) in an attempt to evoke ICMP Time outpace messages from intermediate bound between the scanner and the target host. Standard traceroute employment start with a TTL of 1 and increment the TTL until the destination host is reached. Nmap's traceroute starts with a high TTL and then curtailments the TTL until it reaches zero. Doing it in reverse the Nmap employ clever caching algorithms to accelerate traces over multiple hosts. On relative Nmap sends 5–10 some packets per host, trusting on network conditions. If a single subnet is being scanned (i.e. 192.168.0.0/24) Nmap may only have to send two packets to many hosts.

II TCP port scan layer

TCP port scan layer has various types of scanning such as vanilla, strobe and sweep.

The Vanilla TCP hook-up scan is the most elementary scanning technique. The scan uses the connect system call of an operating system on a destination system to open a connection to every port which is available. The scan is immensely noisy and easily detectable. The targeted system logs will show network requests and error messages for the services that accepted the connections.

Strobe is a network/security tool that discover and describes all listening tcp ports on a (remote) host or on many hosts in a bandwidth utilisation maximising, and the process resource minimising aspect.

Strobe approximates a parallel finite state machine internally. In non-linear multi-host mode it attempts to divide and share the bandwidth and sockets among the hosts very efficiently. This can bring in appreciable growth in speed for multiple distinct hosts/routes.

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to identify which of a range of IP addresses map to live hosts (computers). Whereas a individual ping will tell you whether one stated host computer exists on the network, a ping sweep consists of ICMP (Internet Control Message Protocol) ECHO requests sent to various hosts. If a given address is active, it will reply a message as ICMP ECHO reply. Ping spans are among the older and slower methods used to scan a network.

There are lots of tools that can be used to do a ping sweep, such as fping, gping,and nmapfor UNIX system s, and the Pinger software from Rhino9 and Ping Sweep from SolarWinds for Windows systems. Both Pinger and Ping Sweep send multiple packets at the same time and permit the user to resolve host names and save output to a file.

III Evaluation Layer WGDD

The sensor worm attacks is one of the major hazard to WSN applications. Our wormhole geographic distributed detection (WGDD) algorithm uses a hop counting methodology as a probe procedure. After running the probe procedure, each network node accumulate the set of hop counts of its neighbour nodes that are within one/k hops from it. (The hop count is the minimum number ofnode-to-node transmissions to reach the node from a bootstrap node.) Next, the node runs Dijkstra's (or an equivalent) algorithm to retrieve the shortest path for each pair of nodes, and regenerate a local map using multidimensional scaling (MDS). Finally, a "diameter" feature is used to detect wormholes by classifying misinterpretation in local maps.

The vulnerability Evaluation

The vulnerability assessment evaluates the recovery countermeasures in WSNs against a number of evaluation metrics. Results will reveal if an intrusion recovery countermeasure is exposed to adversaries that launch attacks in order to compromise the deployed recovery. This research work performs the vulnerability assessment in terms of packet delivery

ratio, routing overhead, retransmissions, and number of blocked nodes. Each one of the evaluation metrics will indicate if the deployed recovery countermeasures retain their robustness to adversaries that attack them. Packet delivery ratio will show if the network can reliably deliver packets to the destination in the presence of attacking adversaries. It is measured as the ratio of data packets delivered at destination to those generated by the traffic sources. Routing overhead will demonstrate if the adversary can affect nodes and force the network to trigger the network maintenance operation. The routing overhead is measured as the actual number of routing control packets sent. Each hop-by-hop packet transmission is counted as one transmission. Retransmissions will indicate how severe an attack can be and how it can affect the nodes' effort for packet delivery. The number of blocked nodes will measure the compromisation capabilities of the adversary. In the case of passive attacks, the blocked nodes are calculated by counting the nodes downstream of the malicious nodes and which are prohibited from communicating with the sink. In the case of active attacks, evaluation of blocked nodes considers the nodes downstream of the malicious nodes and its neighbours.

KMP algorithm

Knuth-Morris -Pratt projected a keyword pattern matching algorithm (herein the KMP algorithm) that runs left to right over its text input in linear time and progresses on an algorithm proposed earlier by only Morris and Pratt . This algorithm's pre-computation builds an array with information about how the keyword matches against shifts by itself. For example knowing it have matched exactly r characters around the input permits us to determine that certain shifts are inoperative; thus, avoiding the shifts that the naive brute force algorithm performs only to the fail at a subsequent match attempt. As a detailed example let us say the keyword pattern x = ababaca and we have just matched 5 characters in y starting at position i only to find a disparity for the character c at position i + 5. The naive shift of the brute force algorithm will shift the identical pattern by one location, but of course it would be unsuccessful because the character b at y[i + 1] will not match the first character of the keyword x. The KMP algorithm establish which relevant shift should be, and may shift over multiple positions without missing any potential matches. The disinformation to do this correctly is in the pre-computation step where the prefix function for the keyword is built into an array. Its been defined x as the first r characters of x that have been matched at any point, the prefix function array table at position r (table[r]) contains the extent of object, distance,time of the longest prefix of x that is a proper suffix of x r. Using this information the shift to the next position is always possible to calculate as (the current position) + (the number of matched characters before the mismatch (r)) - (table[r]) . The below Algorithm shows the KMP algorithm and the pre-computation step to prefix function array (table) which is created in time and with memory space O(m).In the worst case the identical phase of the KMP algorithm executes 2n – 1 character comparisons.

Procedure KMP(x, m, y, n)

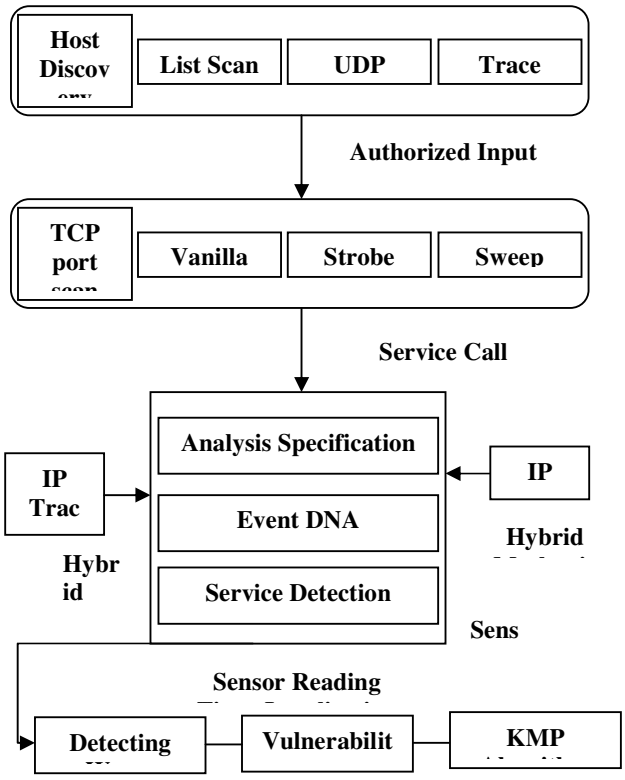
¾ Input:

¾ x ← array of m bytes representing the keyword
¾ m ← integer representing the keyword length
¾ y ← array of n bytes representing the text input
¾ n ← integer representing the text length
table ←Compute Prefix KMP(x, m) // PreComputation
q ← 0
fori = 1 → n do // Matching

```
while q > 0 and x[q + 1] 6 =
y[i] do
 q ← table[q]
end while
if x[q + 1] = y[i] then
 q ← q + 1
end if
if q = m then
outputi – m
 q ← table[q]
end if
end for
end procedure
```

5. SYSTEM ARCHITECTURE

The current trust-based route ways face in getting trust. Energy efficiency is incredibly restricted in WSNs, in most analysis, the trust acquisition and diffusion have high energy consumption, that seriously affects the network lifetime.



6.CONCLUSION

To bring into existence of network clusters in an effective way for improving scalability and longevity of WSN. However, security is a challenging issue in Cluster-based WSNs, since sensors are usually deployed with limited resources in unattended environments. Despite the great efforts in secure clustering of WSN, the dynamic nature of sensor network and numerous possible cluster configurations make searching for a secure and optimal network structure an open challenge. Due to the ability and high secured algorithm Interlock Triple Authentication method becomes a high secured method for data transmission when compared with previous methods.

REFERENCES

1. Liu, A., M. Dong, K. Ota and J. Long, 2015. PACK: AN efficient scheme for selective forwarding attack detection in WSNs. Sensors Journal, 15(12): 30942-30963.
2. Z. Zheng, A. Liu, L. Cai, et al."Energy and Memory efficient Clone Detection in Wireless sensing element networks,"IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp.1130-1143,2016.
3. Lai, C., H. Li, R. Lu and X.S. Shen, 2013. SE-AKA: A secure and efficient cluster authentication and key agreement protocol for LTE networks. laptop Networks, 57(17): 3492-3510.
4. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog optimisation for WSNs," IEEE Transactions on info Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.
5. J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, “Distributed collaborative management for industrial automation with wireless [3] sensor and mechanism networks,” IEEE Trans. Ind. Electron., Vol. 57, No. 12, pp. 4219–4230, Dec. 2010.
6. X. Cao, J. Chen, Y. Xiao, and Y. Sun, “Building-environment management with wireless sensor and mechanism networks: Centralized [4] versus distributed,” IEEE Trans. Ind. Electron.,

Vol. 57, No. 11, pp. 3596–3604, Nov. 2010.

7. R. E. Mezouary, A. Houmz, J. Jalil and M. E. Koutbi, "PRoPHET-RAIP5: a brand new approach to secure routing in wireless sensor networks," 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakech, 2015, pp. 1-6.
8. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in the good grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557-3564, Oct. 2010.
9. And I. Hubaux P. J. and. Knightly W. E, 2008."Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, vol. 16, no. 4, pp. 791- 802, He Q. , Wu D., Sori P. K, 2004.
10. "a secure and objective reputation-based incentive program for ad hoc networks," IEEE Wireless Communications and Networking Conference, pp. 825–830,
11. Akyildiz, IF, Su, W, Sankarasubramaniam, Y &Cayirci, E 2002, 'A survey on sensing element networks', Communications Magazine, IEEE, vol.40, pp.102-114.
12. Michael, L, Raymer, William, F, Punch, Erik, D, Goodman, Leslie, A, Kuhn, & Anil, K, Jain 2000, 'Dimensionality Reduction exploitation Genetic Algorithms,' IEEE Trans. evolutionary Computation, vol.4, no.2, pp.164-171.
13. Yuxin Liu, Mianxiong Dong Ota, Kaoru and Anfeng Liu," ActiveTrust in the Secure and Trustable Routing in Wireless Sensor Networks", IEEE transaction on data forensics and security, Sep 2016, Vol.11, No.9.
14. Jamal N. AI-Karaki, Ahmed E.Kamal,"Routing techniques in wireless sensor networking: A Survey", proceedings by the I-CUBE initiative of Iowa state university, IA 50011,2004.
15. Vipul Sharma, Kirti Patel, Ashish Tiwari "Detection and Suppression of Blackhole Attack in Leach primarily based sensor network", International Journal of technology and Applications, Vol 5 (6),1873-1877, 2014.s