International Journal of Science Engineering and Advance Technology

A Novel DiDrip Protocol with Dissemination-Privilege Pair Authentication

P.Lakshmi Durga[1], Y.Yesu Jyothi[2]
[1]M.Tech Student, Dept of CSE, Srinivasa Institute of Engineering and Technology, Amalapuram, AP.
[2]Assistant Professor, Dept of CSE, Srinivasa Institute of Engineering and Technology, Amalapuram,AP.

ABSTRACT:
It is an attempt to enhance the DiDrip protocol. There are some efficiency problems caused by the generation, transmission, and verification of certificates. First, it is not efficient in communication, as the certificate has to be transmitted along with the advertisement packet across every hop as the message propagates in the WSN. A large per-message overhead will result in more energy consumption on each sensor node. Second, to authenticate each advertisement packet, it always takes two expensive signature verification operations because the certificate should always be authenticated first. Once a new user joins the network after the network deployment, the network owner can notify the sensor nodes of the user's public key/dissemination privilege through using the private key of itself. To enhance secure and distributed data discovery and dissemination protocol (DiDrip), we have planned to use Hop by Hop Message authentication scheme for ensuring data confidentiality.

KEYWORDS: security, wireless sensor networks, efficiency

I. INTRODUCTION:

WSN is conveyed there is normally a need to update buggy old small programs or parameters put away in the sensor nodes. This can be accomplished by the information revelation and dispersal protocol, which offices a source to inject small programs, commands, queries and arrangement parameters to sensor nodes. Note that it is not the same as the code spread conventions which appropriate vast pairs to reinvent the entire system of sensors. For instance, effectively scattering a paired record of several kilobytes requires a code dispersal convention. While scattering a few two-byte setup parameter requires information disclosure and dispersal protocol.

Considering the sensor nodes could be distributed in a harsh situation, remotely spreading such little information to the sensor nodes through the remote channel is a more favored and useful methodology than manual mediation. Persuade by the above perception, this paper as the accompanying fundamental commitment 1 the need of distributed information discovery and dissemination protocol is not totally new, but rather past work did not address this need we concentrate on the useful prerequisite of such convention, and said there configuration objective. Additionally we distinguish the security vulnerabilities in existing information revelation and dissemination protocol.

LITERATURE SURVEY:

[1],we build up a protected and distributed code dissemination protocol named DiCode. A remarkable component of DiCode is its capacity to oppose denial-of-service assaults which have serious outcomes on system accessibility. Further, the security properties of our protocol are exhibited by hypothetical examination. To check the productivity of the proposed approach practically speaking, we additionally actualize the proposed component in a system of asset compelled sensor nodes.

[2], Ensuring that each sensor node has a similar code adaptation is trying in dynamic, temperamental multi-hop sensor nodes. At the point when node have distinctive code forms, the system may not carry on as planned, squandering time and vitality. We propose and assess DHV, a productive code consistency upkeep convention to guarantee that each hub in a system will in the end have a similar code. DHV depends on the simple perception that if two code versions are distinctive, their comparing rendition numbers frequently vary in just a couple of minimum significant bits of their binary representation. DHV permits nodes to deliberately choose and transmit just important bit level data to identify a more up to date code form in the network.

PROBLEM DEFINITION

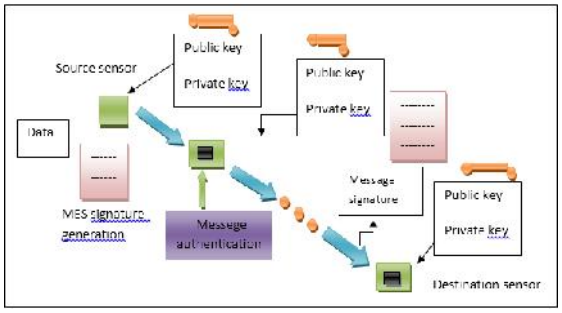
All current information revelation and dissemination protocols employ the brought together approach, information things must be

disseminated by the base station. This methodology experiences the single purpose of failure as spread is outlandish when the base station is not working or when the association between the base station and a node is broken.

PROPOSED APPROACH

We propose secure and information revelation and dissemination protocol (DiDrip). DiDrip comprises of four stages, framework initialization, client joining, and packet preprocessing and packet check. For our fundamental convention, in framework initialization stage, the system proprietor makes its public and private keys, and after that heaps general society parameters on every node before the network deployment.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:
SETTING UP NETWORK MODEL

For our essential convention, in framework initialization stage, the system proprietor makes its open and private keys, and afterward stacks people in general parameters on every node before the system organization. In the client joining stage, a client gets the dissemination benefit through enlisting to the system owner.

SYSTEM INITIALIZATION PHASE

The system owner completes the accompanying strides to determine a private key and some open parameters. it then chooses the private key and registers the general public key. After that, people in general parameters are preloaded in every node of the system.

USER JOINING PHASE

This stage is invoked when a client with the character UID, plans to acquire benefit level. Client picks the private key and registers the general population key. At that point client sends a UID to the system proprietor, where Prij signifies the spread benefit of client. After getting this message, the system owner produces the authentication.

PACKET PRE-PROCESSING PHASE

Expect that a client, enters the WSN and needs to disperse n information things for the development of the packets of the particular information, we have two techniques, i.e., information hash chain and the Merkle hash tree For information hash chain approach, a parcel, is made out of bundle header, and the hash estimation of packet. Here each cryptographic hash is computed over the full packet, not only the information bit, accordingly setting up a chain of hashes.

PACKET VERIFICATION PHASE

At the point when a sensor node, say, gets a packet either from an approved client or from its one-jump neighbours, it first checks the packet'skey field. Looking at the two techniques, the information hash chain strategy causes less correspondence overhead than the Mer-kle hash tree technique. In the information hash chain technique, one and only hash estimation of a packet is incorporated into every packet. Despite what might be expected, in the Merkle hash tree strategy, D(the tree depth) hash qualities are incorporated into every packet.

PERFORMANCE ANALYSIS

For the proposed system, we use the following specific measurements to evaluate its performance:

- Packet Delivery Ratio
- End-to-End Delay
- Packet Loss Ratio

ALGORITHM:
HOP BY HOP MESSAGE ATHENTICATION SCHEME:

Let p > 3 be an odd prime. An elliptic curve E is defined by an equation of the form:

$E: y^2 = x^3 + ac + b mod p,$

Where a, b $\in F_p$, and $4a^3 + 27b^2 \not\equiv 0 \ mod p.$ The set E(F_p) consists of all points (x,y)$\in F_p$on the curve, together with a special point$\mathbf{O}$, called the point at infinity.

Let G = (x_G, y_G) be a base point on E(F_p) whose order is a very large value N. user A selects a random integer $d_A \epsilon$[1, N-1] as his private key. Then, he can compute his public key $Q_A$from $Q_A = d_A \times G$.

SIGNATURE GENERATION ALGORITHM:

For Alice to sign a message m, she follows these steps:

1. Select a random integer k_A,$1 \leq k_A \leq N-1$.
2. Calculate r = $x_A mod$ N, Where (x_A, y_A)= $k_A G$. If r = 0, go back to step 1.
3. Calculate $h_A \overset{l}{\leftarrow} h(m,r)$, where h is a cryptographic hash function, such as SHA-1, and $\overset{l}{\leftarrow}$denotes the l leftmost bits of the hash.
4. Calculate s = r$d_A h_A + k_A$mod N. If s =0, go back to step 2.
5. The signature is the pair (r,s).

SIGNATURE VERIFICATION ALGORITHM:

For Bob to authenticate Alice's signature, he must have a copy of her public key $Q_A$then he:

1. Checks that $Q_A \neq$**O**, otherwise invalid
2. Checks that Q_A lies on the curve
3. Checks that $nQ_A = O$

After that, Bob follows these steps to verify the signature:

1. Verify that r and s are integers in [1, N – 1]. If not, the signature is invalid.
2. Calculate $h_A \overset{l}{\leftarrow} h(m,r)$. where h is the same fucntion used in the signature generation.
3. Calculate (x_1, x_2) = sG - r$h_A Q_A$mod N.
4. The signature is valid if r = x_1 mod N, invalid otherwise.

EXAMPLE:

Elliptic curve equation:$E : y^2 = x^3 + ac + bmodp$

Let us take N=47

Let us take a=2, b=3

And Base point G= (3, 6)

It should satisfy the condition

$4a^3 + 27b^2 \not\equiv 0$

4x (2x2x2) +27x (3x3) =32+243

=275 $\not\equiv 0$

The private key d_A = 31 (Random Integer from [1-46])

The public key

$Q_A = d_A \times G$

Q_A =31x (3, 6)

= (93,186)

1. The random Integer k_A= 17 (Random Integer from [1-46])
2. (x_A, y_A) = 17x (3,6)

= (51,102)

So, x_A =51

r =51%47

=4

3. h_A = 12598 (Generated by SHA-1 algorithm)
4. s =4x31x12598+17%47

= 1562169%47

=30

So the signature is (4, 30)

SIGNATURE VERIFICATION

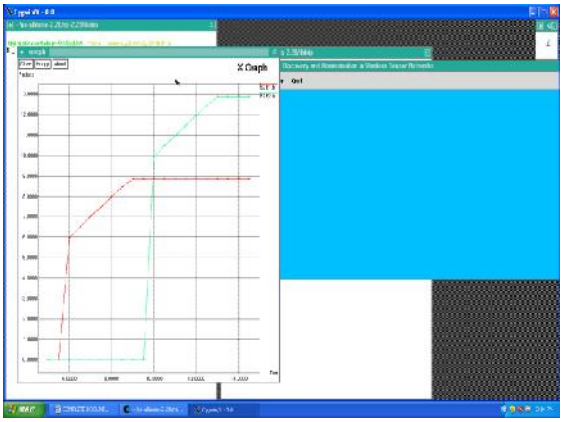
1. Verify r and s value
2. Calculate h_A = 12598 (Generated by SHA-1 algorithm)
3. (x_1, x_2) = 30x(3,6) -4x12598x(93,186) mod 47

= (4, 8)

4. $r = x_1 = 4$

So, Signature is valid

RESULTS:



Simulation result indicate the performance of proposed approach in terms of packet delivery ratio, end-end delay

CONCLUSION:

In this a safe and distributed data discovery and dissemination protocol named DiDrip has been proposed. Other than dissecting the security of DiDrip, this paper has additionally reported the assessment aftereffects of DiDrip in a trial system of asset restricted sensor hubs, which demonstrates that DiDrip is attainable by and by. We have additionally given a formal verification of the realness and honesty of the scattered information things in DiDrip. Likewise, because of the open way of remote channels, Messages can easily intercept. Consequently, later on work, we will consider how to guarantee information privacy in the configuration of secure and conveyed information revelation and dissemination protocols.

FUTURE WORK:

Additionally, because of the open way of remote channels, messages can be effectively blocked. In this way, in the future work, we will consider how to guarantee information classification in the

outline of secure and circulated information disclosure and spread conventions

REFERENCES:

[1] J. W. Hui and D. Culler, "The dynamic behavior of a data disseminationprotocol for network programming at scale," in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst., 2004, pp. 81–94.

[2] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant anddistributed code dissemination in wireless sensor networks,"IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May2012.

[3] T.Dang,N. Bulusu,W. Feng, and S. Park, "DHV:Acode consistencymaintenance protocol for multi-hop wireless sensor networks," inProc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp. 327–342.

[4] G. Tolle and D. Culler, "Design of an application-cooperativemanagement system for wireless sensor networks," in Proc. Eur.Conf. Wireless Sensor Netw., 2005, pp. 121–132.

[5] K. Lin and P. Levis, "Data discovery and dissemination withDIP," in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 2008,pp. 433–444.

[6] M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M.Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildingswith wireless sensor networks: The Torre Aquila deployment," inProc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 277–288.

[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discoveryand dissemination based on hash tree for wireless sensornetworks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638–4646, Sep. 2013.

[8] M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timingsynchronization for heterogeneous sensor networks," in Proc.IEEE Global Telecommun. Conf., 2008, pp. 1–5.

[9] Geoss. [Online]. Available: http://www.epa.gov/geoss/

[10] NOPP. [Online]. Available: http://www.nopp.org/

[11] ORION. [Online]. Available: http://www.joiscience.org/oceanobserving/advisors

[12] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A self-regulatingalgorithm for code maintenance and propagation in wirelesssensor networks," in Proc. 1st Conf. Symp. Netw. Syst. Design
Implementation, 2004, pp. 15–28.

[13] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and securesource authentication for multicast," in Proc. Netw. Distrib. Syst.Security Symp., 2001, pp. 35–46.

[14] Y. Chen, I. Lin, C. Lei, and Y. Liao, "Broadcast authentication insensor networks using compressed bloom filters," in Proc. 4th IEEE Int. Conf. Distrib. Comput. Sensor Syst., 2008, pp. 99–111.

[15] R. Merkle, "Protocols for public key cryptosystems," in Proc. IEEESecurity Privacy, 1980, pp. 122–134.

P.Lakshmi Durga,is a student of Srinivasa Institute of Engineering and Technology, Cheyyeru. Presently she is pursuing her M.Tech [Computer Science And Enggineering] from this college.

Y. Yesu Jyothi,working as Assistant Professor in the Department of CSE in SrinivasaInstitute of Engineering and Technology,Cheyyeru, Katreinakona Mandal EastGodavari District, Andhra Pradesh.