A New Protocol for Mitagate Attacks and Efficient Data Forwading in WSN

[1]M.Padma, [2]T.Veeraju

[1,2]Dept. of CSE, Aditya College of Engineering, Surampalem, E.G.Dt, AP, India

Abstract

A new wireless sensor network is a collection of sensor nodes with limited resources deployed in unattended area updating of old programs and configuration parameters in sensor nodes is essential, for this data discovery and dissemination protocol is required. Existing data discovery and dissemination protocols are not functioning well due to centralized approach and unable to handle attacks launched by attackers. In order to overcome this problem new protocol DiDrip which supports multi-owner and user model .It allows network owners to give authorizations to users along with different privileges for data items forwarding to sensor nodes, another major advantage of this protocol is to handle attacks.

Keywords

Security, Wireless Sensor Networks, Efficiency

I. Introduction

Every current data discovery and dissemination protocols utilize the incorporated approach in which the information items must be spread by the base station. This approach experiences the single purpose of disappointment as scattering is incomprehensible when the base station is not working or when the association between the base station and a node is broken. What's more, the incorporated approach is inefficient, non-adaptable, and defenseless against security attacks that can be propelled anyplace along the correspondence way. Some WSNs don't have any base station by any stretch of the imagination. For instance, for a WSN checking human trafficking in a nation's outskirt or a WSN sent in a remote zone to screen unlawful product development, a base station turns into an appealing focus to be attacked. For such systems, information spread is ideal to be completed by approved system clients in an appropriated way.

II. Literature Survey

[1],we build up a safe and dispersed code dissemination protocol named DiCode. A striking component of DiCode is its capacity to oppose denial-of-service attacks which have extreme outcomes on system accessibility. Promote, the security properties of our protocol are exhibited by hypothetical examination. To check the productivity of the proposed approach by and by, we additionally actualize the proposed component in a system of asset constrained sensor nodes.

[2], we propose and assess DHV, an effective code consistency upkeep protocol to guarantee that each node in a system will in the end have a similar code. DHV depends on the basic perception that if two code versions are distinctive, their comparing version numbers frequently vary in just a couple of slightest huge bits of their binary representation. DHV permits nodes to precisely choose and transmit just fundamental bit level data to distinguish a more up to date code version in the system. DHV can recognize and distinguish version contrasts in O(1) messages and latency contrasted with the logarithmic size of current protocols.

III. Problem Definition

All the more imperatively, 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.

IV. 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.

V. System Architecture

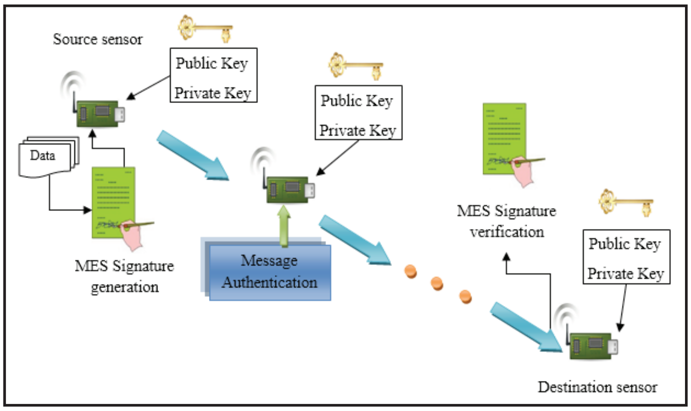

Fig. 1:

VI. Proposed Methodology

A. Setting Up Network Model

System comprises of four stages, framework initialization, client joining, and packet pre-preparing and packet check. 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.

B. System Initialization Phase

In this stage, 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.

C. 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.

D. 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.

E. Packet Verification Phase

At the point when a sensor hub, say, gets a packet either from an approved client or from its one-jump neighbors, it first checks the packet'skey field. Looking at the two techniques, the information hash chain strategy causes less correspondence overhead than the Merkle 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.

F. Performance Analysis

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

1. Packet Delivery Ratio
2. End-to-End Delay
3. Packet Loss Ratio

VII. Algorithm:

Hop By Hop Message Authentication Scheme:

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

$$E{:}y^2 = x^3 + ac + b\text{mod}p,$$

Where a, b ∈ F_p, and $4a^3 + 27b^2 \not\equiv 0$ modp. The set $E(F_p)$ consists of all points $(x,y)\in F_p$ on the curve, together with a special pointO, 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 $s = rd_A h_A + k_A$ 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 n $Q_A = O$

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 $(x_1, x^2) = sG - rh_A Q_A$ mod N.
4. The signature is valid if $r = x_1$ mod N, invalid otherwise.

Example:

Elliptic curve equation: $E{:}y^2 = x^3 + ac + b\text{modp}$
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 ≢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. $r = x_1 = 4$

VIII. Results

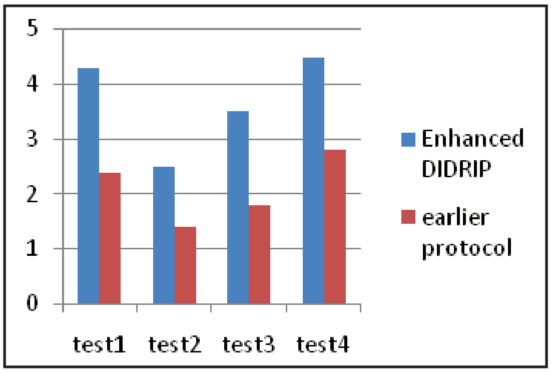

Fig. 2:

The simulation results are generated by using java swings and socket programming.Finally proposed enhanced didrip protocol shows efficiency in secure data communication.

IX. Conclusion

We have distinguished the security vulnerabilities in information revelation and dissemination when utilized as a part of WSNs, which have not been tended to in past research. Additionally, none of those methodologies support distributed operation. Accordingly, in this a safe and dispersed information revelation and dissemination protocol named DiDrip has been proposed. Other than breaking down the security of DiDrip, in this we reported the assessment consequences of DiDrip in an exploratory system of asset constrained sensor nodes, which demonstrates that DiDrip is achievable practically speaking.

X. 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, D. Culler,"The dynamic behavior of a data dissemination protocol for network programming at scale," In Proc. 2ndInt. Conf. Embedded Netw. Sensor Syst., 2004, pp. 81–94.

[2] D. He, C. Chen, S. Chan, J. Bu,"DiCode: DoS-resistant anddistributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., Vol. 11, No. 5, pp. 1946–1956, May 2012.

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

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

[5] K. Lin, 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, 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, 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, T. Taleb,"Pairing-based secure timingsynchronization for heterogeneous sensor networks," In Proc. IEEE Global Telecommun. Conf., pp. 1–5, 2008.

[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, S. Shenker,"Trickle: A self-regulatingalgorithm for code maintenance and propagation in wirelesssensor networks," In Proc. 1st Conf. Symp. Netw. Syst. Design Implementation, pp. 15–28, 2004.

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

[14] Y. Chen, I. Lin, C. Lei, Y. Liao,"Broadcast authentication insensor networks using compressed bloom filters," In Proc. 4thIEEE 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.

M PADMA is a student of Aditya College of Engineering, Surampalem. Presently She is pursuing herM.Tech [Computer Science Engineering] from this college and she received his B.Tech from Sri Sai Aditya institute of Science & Technology, affiliated to JNT University, Kakinada in the year 2013. Her area of interest includes Computer Networks and Object Oriented Programming Languages, all current trends and techniques in Computer Science.

T.VEERAJU, well known Author and excellent Teacher in M.Tech (CSE) in AdityaCollege of Engineering .He has 17 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals. His area of Interest includes Data Warehouse and Data Mining, information security and other advances in computer Applications.