Low Priced and Energy Economical Detection of Replicas for Wireless Sensor Network

Dhope Ankita Sanjay[1], Tupe Komal Ankush[2], Pise Pooja Dnyaneshwar[3]

Department of Computer Science and Engineering, Shriram Institute of Engineering and Technology Center, Paniv Tal: Malshiras, Dist: Solapur, Pin Code: 413113

---***---

Abstract - *The forthcoming net of things—an intelligent collaboration of resource-limited devices like wireless sensing element nodes that area unit embedded within the daily lives of users—poses new challenges to security and end-user privacy. One amongst the foremost difficult issues is that the thwarting of reproduction attacks. Once a sensing element node is physically captured, it may be reprogrammed and replicated into an outsized range of replicas, which can maliciously occupy the network. Thus far, varied schemes are planned to notice replicas; but, most of them need high-ticket hardware like a world positioning system. In general, the best value for a sensing element node is as low together dollar, and thus, it's equipped with restricted resources; therefore, it's not sensible to use further devices. During this paper, we have a tendency to propose a inexpensive and economical resolution for reproduction detection in static wireless sensing element networks. Though the planned resolution doesn't want any further hardware, it exhibits similar or higher performance, as compared to existing schemes. Through simulation experiments, we have a tendency to show that the planned resolution provides comparable performance in terms of the reproduction noticeion magnitude relation and therefore the time needed to detect replicas. Moreover, we have a tendency to show that the planned resolution saves a lot of energy than existing schemes in most of our simulations.*

Key Words**: Security, Protection, Authentication, Network Protocol, Bloom Filter, Ubiquitous Computing**

1. INTRODUCTION

Wireless device network are provides 2 completely different technologies such as: computation and communication. It consists of enormous variety of sensing devices conjointly support for: Physically and Environmental conditions like: humidness, Temperature, Pressure, Sound etc. Data collected by sensing devices and conjointly transmitted to the destination .It conjointly called base station or sink. WSN's have varied security challenges as compared to ancient network. The device nodes typically support for tamper resistances behind the hardware. It conjointly unfolds in insecure environments. Wherever they're not grunted to capture and compromise attack. These replicas may be used for varied launch concealing attack betting on the attacker's motives. The like listen in secret to non-public on network communication or dominant the supply areas. This kind of attack is additionally called "Replica attack". Accordingly, while not mistreatment hardware like: GPS, we have a tendency to style low value duplicate detection resolution for static wireless device network by mistreatment "Bloom Filter" and "Sequential delivery algorithm". Neighbour nodes IDs conjointly given with constant size by mistreatment Bloom Filter. "Bloom Filter Output" (BFO): uses for proof. The during this ways slowly increase traffic between the neighbour node and at random chosen nodes ,then exiting system generates significant traffic by sending proofs kind the beginning. The complete result shows that the planned resolution is a lot of energy economical than exiting system. The contribution of purposed resolution as follows: low value solution:

1) The planned solution conjointly reduces the value of building wireless device Network duplicate detection. 2) Economical - energy detection: energy potency is very important in wireless device network. We have a tendency to think about node in setting are typically non reversible and thence convenience depends on energy potency support for giant scale.

1.1 System Architecture

The planned system supply a security in network system, named inexpensive and Energy-Efficient Detection of Replicas for Wireless detector Networks, discover duplicate node for static wireless detector network.

We planned an occasional priced and energy-efficient solved to discover duplicate node for static wireless detector network planned doesn't use any further hardware. Wherever existing system want of costly hardware like as GPS receiver. Planned answer use exhibits duplicate node or smart performance than existing theme. Once one or additional replicas detects at intervals the short length time and increase the high performance additionally gain the less energy.

Main parts needed for low worth economical energy reproduction detection in WSN, climatically sensors, wireless communication, Broadcast (network to node). In our system style, climatically parameters square measure scan from nearest automatic observation post and square measure interpolated to suit the native climate.

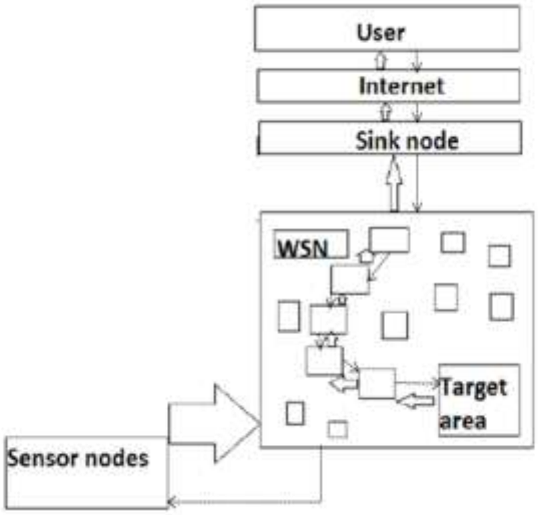

Fig: System Architecture

1.2 Modules

1. Node Formation

Neighboring node IDs area unit bestowed with a continuing size employing a Bloom filter. The Bloom filter output (BFO) is employed as a symbol. A new deployed node generates completely different proofs consistent with the collected neighboring node IDs, till assembling the whole neighboring node IDs. The proofs area unit delivered to a at random elite node within the network. Here, the delivery frequency will increase proportionately to the amount of the collected neighboring node IDs. The strategy slowly will increase traffic between the neighboring nodes and their at random elite nodes;

2. Find Attacker:

With respect to this attack, it's assumed that associate offender captures solely atiny low fraction of nodes within the network as a result of capturing an outsized fraction might not need replicas to any extent further, and it's going to be additional expensive and detectable. It's affordable to assume that associate offender captures solely a number of nodes and obtains secret info from the captured nodes. Then the offender makes replicas by storing secret info during a sizable amount of trade goods device nodes. The replicas area unit equally deployed within the network therefore on reach his/her objectives, like eavesdropping on network communications or dominant the target areas. Since the offender already is aware of the key info of the captured node, it's futile to use existing cytological solutions, within which their security depends on the key info.

3. Replica Attack and Detection Using Bloom Filter:

An aggressor captures one or a lot of nodes deployed within the network then obtain secret data from them. Next, the aggressor makes multiple replicas by mistreatment this data then deploys them into targeted areas. Here, the neighboring nodes acknowledge replicas as recently deployed nodes. For getting helpful data from the neighboring nodes within the target areas or dominant the neighboring nodes, replicas ought to prove that they're legitimate nodes with valid secret data. However, since replicas already recognize the key data, they'll prove it to the neighboring nodes without problems.

4. Validation of Node:

The RDB-R consists of 3 stages: proof generation, proof delivery, and proof validation. Henceforth, we tend to make a case for the 3 stages with new preparation node A, the neighboring node C, and therefore the witness node U. within the initial Stage a symptom for distinguishing a duplicate is made and updated in an exceedingly freshly additional node A , which can be a duplicate. Second Stage, checks whether or not neighboring node IDs area unit registered to a symptom (i.e., BFOA) or whether or not the received IDs belong to a two-hop neighbor list. In finish is to see whether or not the supply node, that may be a node generating the proof, may be a reproduction through a set checking technique.

2. Algorithm

A Bloom filter is a memory-efficient, probabilistic data structure that we can use to answer the question of whether or not a given element is in a set. There are no false negatives with a Bloom filter, so when it returns false, we can be 100% certain that the element is not in the set. However, a Bloom filter can return false positives, so when it returns true, there is a high probability that the element is in the set, but we can not be 100% sure. The Bloom filter is designed to be space-efficient and fast. When using it, we can specify the probability of false positive responses which we can accept and, according to that configuration, the Bloom filter will occupy as little memory as it can. Due to this space-efficiency, the Bloom filter will easily fit in memory even for huge numbers of elements. Some databases, including Cassandra and Oracle, use this filter as the first check before going to disk or cache, for example, when a request for a specific ID comes in. If the filter returns that the ID is not present, the database can stop further processing of the request and return to the client. Otherwise, it goes to the disk and returns the element if it is found on disk.

3. CONCLUSION

In this paper, we proposed a low-cost efficient solution to detect replicas for static WSNs. The proposed solution does not need any additional hardware, whereas existing schemes require expensive hardware such as a GPS receiver.

Nevertheless, the proposed solution generally exhibits similar or better performance than existing schemes; it detects more replicas within a shorter time while consuming less energy. This means that we can develop an efficient replica detection system for WSNs at a considerably lower cost.

REFERENCES

[1] C.P. Mayer, "Security and Privacy Challenges in the Internet of Things, Electronic Comm. EASST, vol. 17, pp. 1-12, 2009.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Survey Internet of Things: Vision, Applications and Research Challenges," J. Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, Sept. 2012.

[3] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, 2005.

[4] M. Conti, R.D. Pietro, L. Mancini, and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 5, pp. 685-698, Sept. 2011.

[5] C.A. Melchor, B. Ait-Salem, and P. Gaborit, "Active Detection of Node Replication Attacks," Int'l J. Computer Science and Network Security, vol. 9, no. 2, pp. 13-21, 2009.

[6] H. Choi, S. Zhu, and T.F.L. Porta, "Set: Detecting Node Clones in Sensor Networks," Proc. Third Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.

[7] Z. Li and G. Gong, "DHT-Based Detection of Node Clone in Wireless Sensor Networks," Proc. First Int'l Conf. Adhoc Networks, pp. 240-255, 2009.

[8] K. Xing, F. Liu, X. Cheng, and D.H.C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," Proc. 28th Int'l Conf. Distribute Computing Systems (ICDCS '07), pp. 3-10, 2008.

[9] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks," IEEE J. Selected Areas Comm., vol. 28, no. 5, pp. 677-691, June 2010.

[10] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks," IEEE Trans. Mobile Computing, vol. 9, no. 7, pp. 913-926, July 2010.

BIOGRAPHIES

Ms. Dhope Ankita Sanjay is currently pursuing B.E (Computer) from Dept of Computer Science & Engineering, Shriram Institute of Engineering and Technology Center, Paniv. She received her Diploma (Computer Technology) from Shriram institute of Engineering & technology (Poly.), Paniv. Her area of interest is Network Security.

Ms. Tupe Komal Ankush is currently pursuing B.E (Computer) from Dept of Computer Science & Engineering, Shriram Institute of Engineering and Technology Center, Paniv. She received her Diploma (Computer Technology) from Shriram institute of Engineering & technology (Poly.), Paniv. Her area of interest is Network Security.

Ms. Pise Pooja Dnyaneshwar is currently pursuing B.E (Computer) from Dept of Computer Science & Engineering, Shriram Institute of Engineering and Technology Center, Paniv. She received her Diploma (Computer Technology) from Karmayogi Polytechnic College Shelve Pandharpur. Her area of interest is Network Security.

Ms. Hande Priti Navanath is currently working as a Assistant Professor in Solapur University (S.I.E.T.C., Paniv) having 1.5 year experience of teaching. She received her M.E(Computer Science And Engineering) from JSCOE .She received her B.E(Computer Science And Engineering) from DYPIET . Her area of interest is Network Security.