Detection and Prevention of Sybil Attacks in Mobile Wireless Sensor Networks

Preeti , Poonam Chaudhary

Abstract— **Due to broadcast nature of Wireless Sensor Networks (WSNs) and lack of tamper-resistant hardware, security in sensor networks is one of the major issues. Hence research is being done on many security attacks on wireless sensor networks. Wireless Sensor Networks are rapidly gaining interests of researchers from academia, industry, emerging technology and defence. This paper focuses on Sybil method and its detection. When a node illegitimately claims multiple identities or claims fake id, is called Sybil attack. An algorithm is proposed to detect the Sybil attack.**

Keywords **— Wireless Sensor Network (WSN), Sybil Attack.**

I. INTRODUCTION

WSN is becoming increasingly popular due to the variety of applications. It is widely used in the field of education, military, medical treatment, traffic, and has huge potential and commercial value. In WSN, there are thousands of nodes deployed in severe environment to collect information such as light intensity, pressure and temperature, or detect danger and track of enemy. Sensor node is typically low-cost, battery powered; highly resource constrained and usually collaborates with each other to accomplish a task. So it is more vulnerable in the face of security threats than wired network [1].

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder. The name was suggested in or before 2002 by Brian Zill at Microsoft Research. The term "pseudo spoofing" had previously been coined by L. Det weiler on the Cypher punks mailing list and used in the literature on peer-to-peer systems for the same class of attacks prior to 2002, but this term did not gain as much influence as "Sybil attack".

In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. Evidence shows large-scale Sybil attack can be carried out in a very cheap and efficient way in realistic systems like Bit Torrent Mainline DHT.

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally. External attacks can be prevented by authentication but not the internal attacks. There should be one to one mapping between identity and entity in WSN. But this attack violates this one-to-one mapping by creating multiple identities. [2]

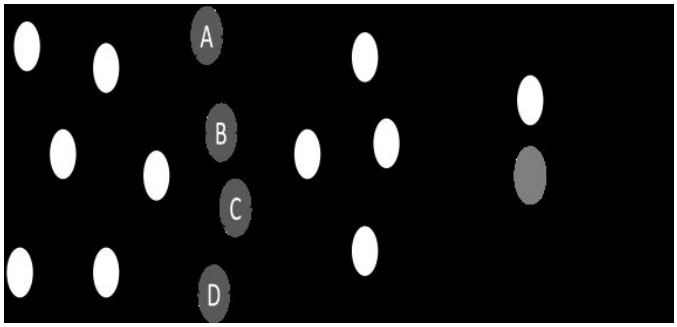

Figure: Sybil Attack

II. RELATED WORK

. *A. Security Concepts and Sybil Attack Detection in Wireless Sensor Networks* Due to broadcast nature of Wireless Sensor Networks (WSNs) and lack of tamper-resistant hardware, security in sensor networks is one of the major issues. Hence research is being done on many security attacks on wireless sensor networks. Wireless Sensor Networks are rapidly gaining interests of researchers from academia, industry, emerging technology and defence. WSNs consist of a large number of sensor nodes and a few sink nodes or base station are deployed in the field to gather information about the state

Manuscript received July, 2015.

Preeti*, Department of Electronics and Communication Engineering, Prannath Parnami Institute of Management and Technology. Hisar,Haryana India*

Poonam Chaudhary*, Department of Electronics and Communication Engineering, Prannath Parnami Institute of Management and Technology. Hisar,Haryana India*

of physical world and transmit it to interested users, typically used in applications, such as, habitat monitoring, military surveillance, environment sensing and health monitoring. Sensor nodes have limited resources in term of processing power, battery power, and data storage. When a node illegitimately claims multiple identities or claims fake id, is called Sybil attack. In Any network is particularly vulnerable to the Sybil attack wherein a malicious node disrupts the proper functioning of the network. Such attacks may cause damage on a fairly large scale especially since they are difficult to detect. This paper focuses on various security issues, security threats, Sybil attack and various methods to prevent Sybil attack.[3]

B. Detection of Sybil attack in mobile wireless sensor networks Security of Wireless sensor networks is one of the major issues; hence research is being done on many routing attacks on wireless Sensor networks. This paper focuses on Sybil method and its detection. When a node illegitimately claims multiple identities or claims Fake id, is called Sybil attack. An algorithm is proposed to detect the Sybil attack. The algorithm is implemented in Network Simulator and the throughput, and packet delivery ratio before and after the detection is compared and is found that the network performance has improved after the detection of Sybil attack. [4]

C. A Lightweight Key Establishment in Wireless Sensor Network Based on Elliptic Curve Cryptography
Recently, there have been a lot of researches and Technological advances about using Public Key Cryptography (PKC) in wireless sensor network (WSN), which demonstrates that it is feasible to WSN. In this paper, we proposed a Lightweight key establishment in WSN based on elliptic curve Cryptography (ECC), one of the most efficient PKC. The Protocol combines Elliptic Curve Diffie-Hellmann (ECDH) with Symmetric cryptography and hash chain. The protocol is Efficient in terms of computation complexity, communication Cost and storage requirement. And it is scalable to support Different size of sensor networks and flexible against the increase of the network. Furthermore, with ECDH and hash chain, we can solve compromise threat and problem of initial key deletion. Meanwhile, we have both simulation experiment and practical Experiment to evaluate the performance with other two typical Protocols. It turns out that our protocol is more efficient than other public key schemes. [5]

D. Security in Wireless Sensor Networks with Public Key Techniques Wireless sensor networks (WSNs) have attracted a lot of researchers due to their usage in Critical applications. WSN have limitations on Computational capacity, battery etc which provides Scope for challenging problems. Applications of WSN are drastically growing from indoor deployment to Critical outdoor deployment. WSN are distributed and Deployed in an unattended environment, due to this WSN are vulnerable to numerous security threats. The Results are not completely trustable due to their Deployment in outside and uncontrolled environments. In this current paper, we fundamentally focused on these security issues of WSNs and proposed a protocol Based on public key cryptography for external agent Authentication and session key establishment. The Proposed protocol is efficient and secure in compared to other public key based protocols in WSNs [6]

III. OBJECTIVE

Validation techniques may be accustomed stop Sybil attacks and dismiss masquerading hostile entities. an area entity might settle for a foreign identity supported a central authority that ensures a matched correspondence between associate degree identity associate degreed an entity and should even offer a reverse search. associate degree identity is also valid either directly or indirectly. In direct validation the native entity queries the central authority to validate the remote identities. In indirect validation the native entity depends on already accepted identities that successively vouch for the validity of the remote identity in question.
Identity-based validation techniques usually offer answerableness at the expense of namelessness, which might be associate degree undesirable exchange particularly in on-line forums that would like to allow censorship-free info exchange and open discussion of sensitive topics. A validation authority will plan to preserve users\' namelessness by refusing to perform reverse lookups, however this approach makes the validation authority a major target for attack. as an alternative, the authority will use some mechanism apart from information of a user\'s real identity - like verification of associate degree unidentified person\'s physical presence at a specific place and time - to enforce a matched correspondence between on-line identities and real-world users.

Sybil hindrance techniques supported the property characteristics of social graphs can even limit the extent of injury which will be caused by a given Sybil assailant whereas protective namelessness, tho\' these techniques cannot stop Sybil attacks entirely, and should be at risk of widespread small-scale Sybil attacks. samples of such hindrance techniques area unit Sybil Guard and therefore the Advogato Trust Metric. And additionally the scantiness primarily {based} metric to spot Sybil clusters during a distributed P2P based name system.

IV. METHODOLOGY/ PLANNING

- Deploy nodes in an area in random fashion
- Select a sender and receiver
- information will travel from sender to receiver
- but now, the sender node will only send data to the next node in its range
- and also, there will be an attacker which is randomly moving in the whole scenario
- if, in any case, while sender is transmitting to the receiver, the attacker comes in the range of sender, the information will be leaked
- so the scenario will continue to run until such an error occurs
- We will deploy an authentication mechanism with which the attacker cannot disguise any genuine node and could steal the information.

ISSN: 2278 – 1323

V. Implemented Results and Discussion

Following are the results (screenshots) of one of the scenario that we ran.

1. We will start by entering the number of sensors we would like to take part in the scenario and we will also enter the proposed range of each sensor

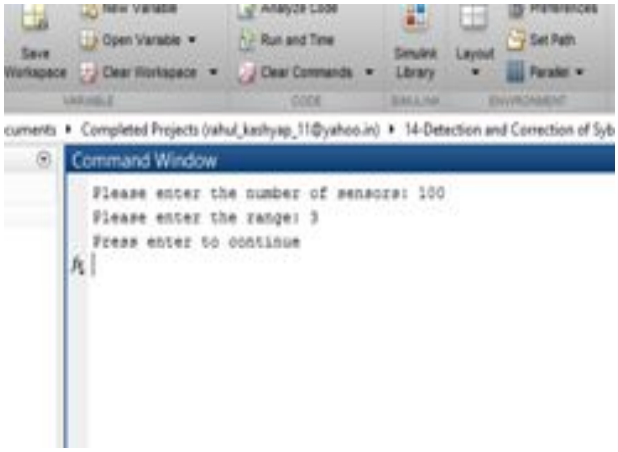

Figure 2: Entering Number of Sensors

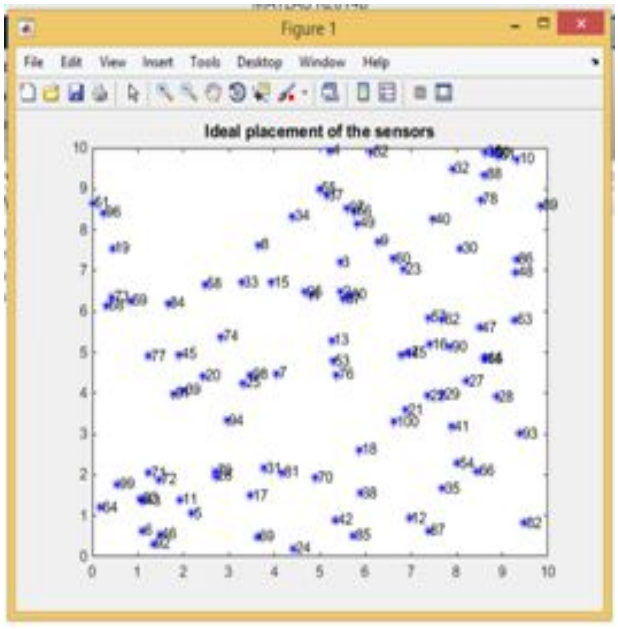

Figure 3: Placement of Sensor Nodes

2. Next, we have to enter the sender node and receiver node. We have to transmit the information from sender to receiver
3. We will first run the scenario with errors (default scenario). In this process, sender will try to send information to receiver (within its range). But once we encounter an attacker in the range, our information will be attacked. The scenario will stop due to this.

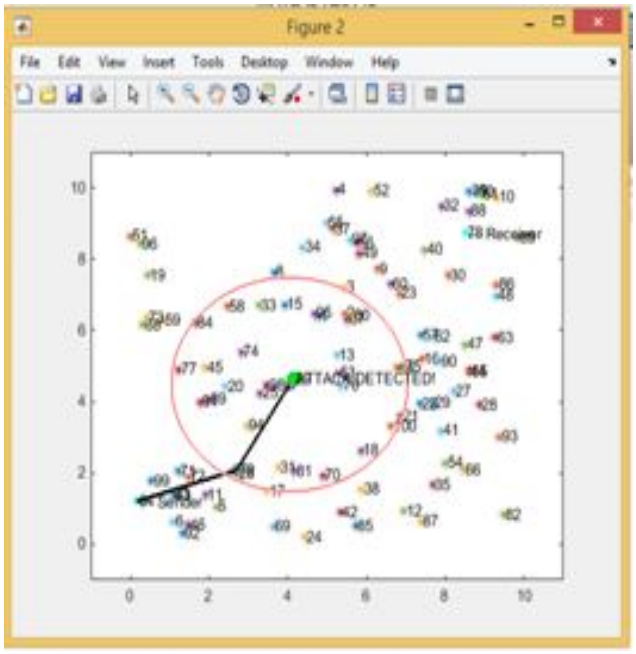

Figure 4: Default Scenario

4. We can perform the above scenario repetitively and could check how many times we encounter an attacker. We can run this scenario multiple number of times. We just have to select "Y"
5. And we will start the scenario without errors, which is the proposed scenario

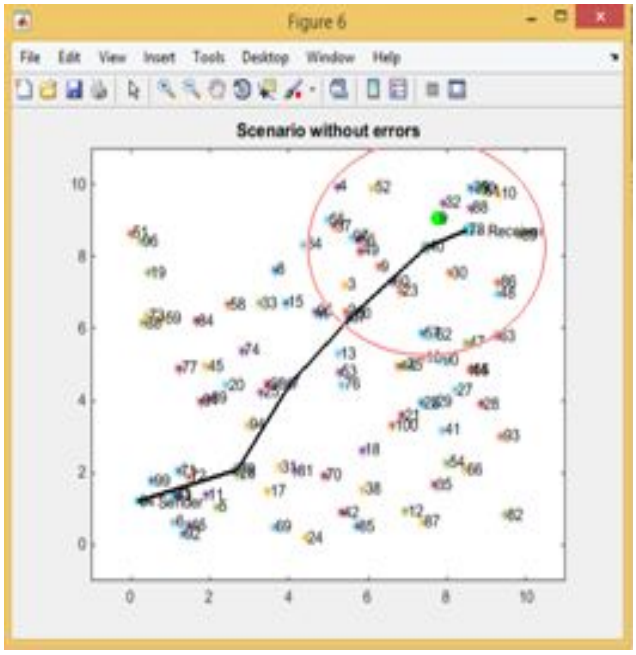

Figure 5: Scenario without Error

In this scenario, even if we get any attacker in the range, our information will not be sacrificed and it will reach its destination safely. We can again run this scenario multiple times, until we have packets left to send.

Yet again, the program will run until all the packets are exhausted. Following are the results that we calculated on the basis of above simulation.

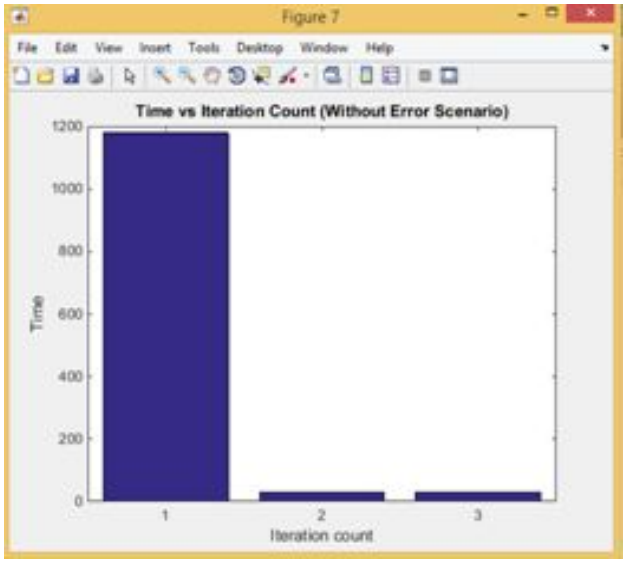

Figure 6: Time Vs Iteration Count

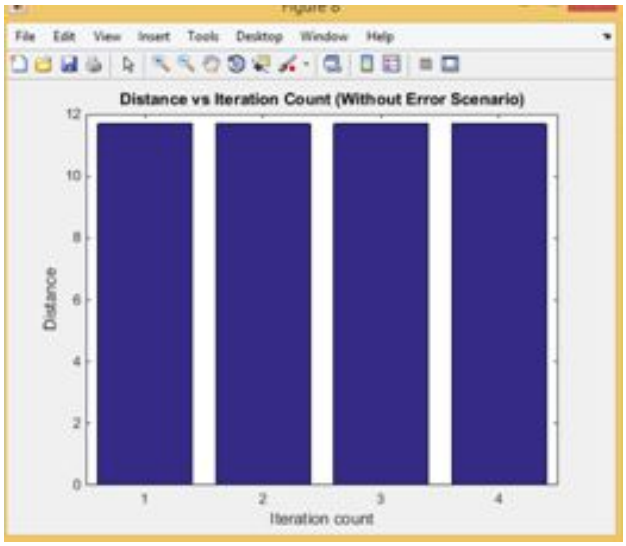

Figure 7: Distance Vs Iteration Count

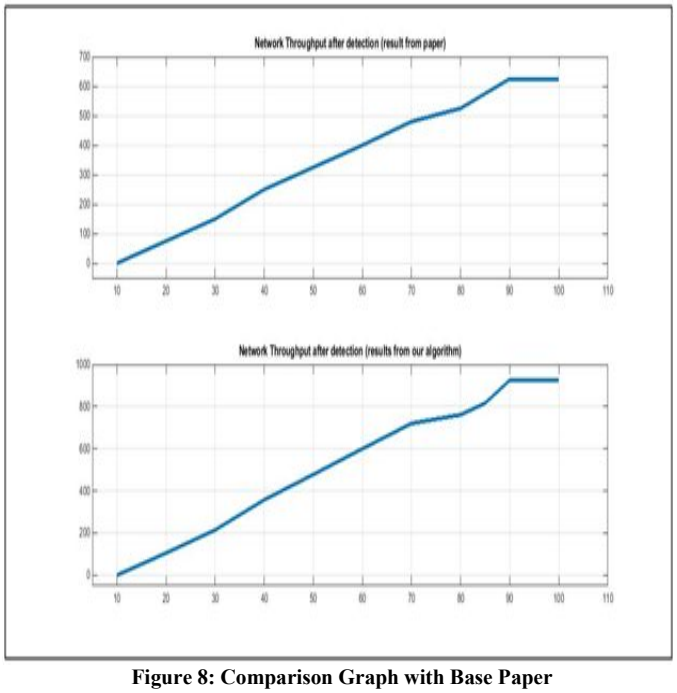

Figure 8: Comparison Graph with Base Paper

VI. CONCLUSION

We have presented the general concept ofWireless sensor network and security in wireless sensorNetwork. Current research so far focuses on theSecurity of wireless sensor network. Our scheme improves the security level of WSN. Moreover, our scheme isScalable and flexible. Hence, we could successfully conclude that attack of Sybil nodes were prevented and network throughput was increased using the proposed work.

REFERENCES

[1] H. Chan and A. Perrig, "*Security and Privacy in Sensor Networks*" IEEE Computer,Vol. 36(10), October 2003, pp. 103-105.
[2] J.R. Douceur. The Sybil attack. In First International Workshop on Peer-to Peer Systems (IPTPS'02), Mar. 2002.
[3] *Manjunatha T. N1, Sushma M. D2, Shivakumar K. M3 "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks" IJETTS, Volume 2, Issue 2, March – April 2013.*
[4] *SelfS.Sharmila1, G Umamaheswari2 "Detection of Sybil Attack In Mobile Wireless Sensor Networks" [IJESAT], Volume-2, Issue-2, 256 – 262.*
[5] Song Ju, "*A Lightweight Key Establishment In Wireless Sensor Network Based On Elliptic Curve Cryptography*" Beijing, China
[6] 1Vorugunti Chandra Sekhar, 2Mrudula Sarvabhatla, "*Security In Wireless Sensor Networks With Public Key Techniques*" (ICCCI -2012), Jan. 10 – 12, 2012, Coimbatore, INDIA.
[7] akshai aggarwal, savita Gandhi and nirbhay chaubey "*a study of secure routing protocol in mobile ad hoc networks*" in proceedings of national conferences on advancement in wireless technology and applications, 18-19 december 2008,SVNIT,Surat,India.
[8] Qiu Hui-Min. "*Principle of Sybil attack and the defence*" Network and Computer Security, vol 10, pp.63-65, October 2005.
[9] S.Abbas, M.Merabti, and D.Llewellyn-Jones. *Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks*. Second International Conference on Developments in eSystems Engineering, 2009.
[10] J. Newsome, E. Shi, and D. Song, "*The Sybil Attack in Sensor Network: Analysis & Defences*," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, California, USA: ACN Press, 2004, pp.185-191
[11] Z. Qinghua, W. Pan, S. Douglas, and P Ning, "*Defending against Sybil attacks in sensor networks,*" Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshop (ICDCSW'05), 2005, pp.185-191
[12] L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming, "*Detecting the Sybil Attack Cooperatively in Wireless sensor Networks*," in International Conference on Computational Intelligence and Security, CIS '08. Vol.1 2008, pp.442-446

ISSN: 2278 – 1323

BIOGRAPHICS

Preeti recived the B.Tech. And M.Tech. Degree in Electronics and instrumentation Engineering and Electronics and Communication Engineering from K.U.K. University and GJU&ST University. Her research interest include Wireless networks and security.

Poonam Choudhary received degree of B.E in Electronics and Communication from Rajasthan University, Jaipur and degree of M.Tech from GJU&ST, Hisar, India in 2006 and 2013 respectively. She is now teaching as an Assistant professor in ECE, department in PPIMT, Hisar.

