International Journal of Science Engineering and Advance Technology

A Novel Approach For Secure Scheme Of Detecting Data Provenance And Packet Drop Attacks In Sensor Networks

Syed Gulam Gouse[1], Dr.R.Kiran Kumar[2]
[1]Assistant Professor, Dept of CSE, Nimra College of Engineering and Technology, A.P., India.
[2]Co.Ordinator, Center Of Research Studies, Krishna University, A.P., India.

Abstract — Sensor networks are utilized as a part of various application spaces, for example, digital physical framework frameworks, natural checking, control lattices, and so on. Information are created at an extensive number of sensor hub sources and handled in-organize at middle of the road jumps on their way to a Base Station (BS) that performs basic leadership. The assorted variety of information sources makes the need to guarantee the reliability of information, to such an extent that lone dependable data is considered in the choice procedure. Information provenance is a successful strategy to evaluate information reliability, since it outlines the historical backdrop of proprietorship and the activities performed on the information. Information provenance speaks to a key factor in assessing the reliability of sensor information. Provenance administration for sensor systems presents a few testing necessities, for example, low vitality and transfer speed utilization, effective capacity and secure transmission. In this paper particular commitments are:

• Formulate the issue of secure provenance transmission in sensor organizes, and distinguish the difficulties particular to this unique circumstance;

• Propose an in-parcel Bloom channel provenance encoding plan;

•Design proficient procedures for provenance unraveling and confirmation at the base station;

• Extend the safe provenance encoding plan and devise a system that identifies bundle drop assaults arranged by vindictive sending sensor hubs;

• Perform a point by point security investigation and execution assessment of the proposed provenance encoding plan and parcel misfortune recognition component.

Keywords **—Security, Sensor Network, Bloom Filtering, Encryption.**

1. INTRODUCTION

Sensor network is the proficient social occasion and transmission of detected information to a base station for propel preparing. The life of such a sensor framework is the time amid which it can assemble data from every one of the sensors to the base station. An essential test in information gathering is to boost the framework lifetime, given the vitality requirements. As sensor systems are as a rule all the time more sent in basic leadership the procedure that on in bundle Bloom channels to encode provenance of the data. This proposed work presents proficient instruments for provenance confirmation technique and reproduction strategy at the base station with the usefulness to distinguish bundle drop assaults or by noxious information sending hubs. Late research featured the key commitment of provenance in frameworks where the utilization of conniving information may prompt calamitous disappointments (e.g., SCADA frameworks). In spite of the fact that provenance displaying, gathering, and questioning have been considered broadly for work processes and made databases, provenance in sensor systems has not been legitimately tended to. We explore the issue of secure and proficient provenance transmission and handling for sensor systems, and we utilize provenance to identify bundle misfortune assaults organized by pernicious sensor hubs. In a multi-jump sensor organize, information provenance enables the BS to follow the source and sending way of an individual information parcel. Provenance must be recorded for every parcel, except vital difficulties emerge because of the tight stockpiling, vitality and data transmission limitations of sensor hubs. In this way, it is important to devise a light-weight provenance arrangement with low overhead. Besides, sensors frequently work in an untrusted domain, where they might be liable to assaults. Consequently, it is important to address security prerequisites, for example, privacy, uprightness and freshness of provenance. We will likely plan a provenance encoding and unraveling component that fulfills such security and execution needs. We propose a provenance encoding technique whereby every hub on the way of an information parcel safely installs provenance data inside a Bloom channel that is transmitted alongside the information. After accepting the bundle, the BS removes and checks the provenance data. We likewise devise an augmentation of the provenance encoding plan that enables the BS to distinguish if a bundle drop assault was arranged by a malevolent hub. Instead of existing exploration that utilizes isolate transmission channels for

information and provenance, we just require a solitary channel for both. Moreover, customary provenance security arrangements utilize seriously cryptography and advanced marks, and they utilize attach based information structures to store provenance, prompting restrictive expenses. Conversely, we utilize just quick Message Authentication Code (MAC) plans and Bloom channels (BF), which are settled size information structures that minimally speak to provenance. Blossom channels make proficient utilization of transfer speed, and they yield low blunder rates practically speaking.

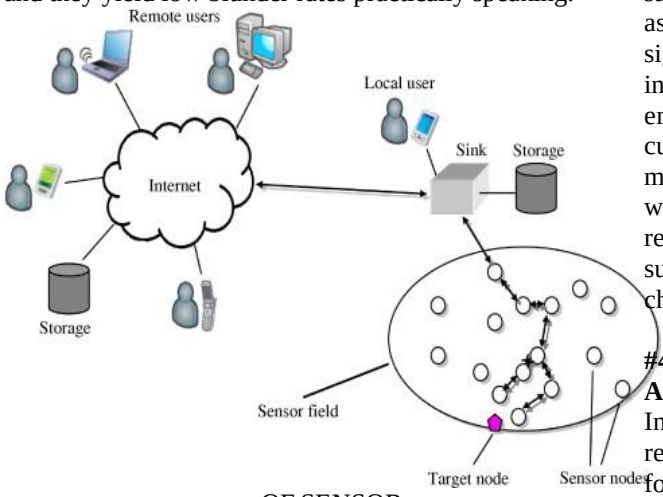


FIG: GATEWAY OF SENSOR NETWORK

2. LITURATURE SURVEY

Wenchao Zhou [1] et.al watched the need of securing the provenance data and proposed a plan named, Secure Network provenance which gives evidence for the condition of the provenance information. System administrator can recognize defective hubs and furthermore can survey the harm to arrange from such flawed hubs. Snoopy named SNP is proposed in paper and exploratory outcomes demonstrated that Snoopy can demonstrate condition of provenance information in vindictive WSN display. SNP conspire did not consider the impediments of WSN i.e. constrained transmission capacity, low battery and low memory.

#2 Access points vulnerabilities to DoS attacks in 802.11 networks

We depict conceivable dissent of administration assaults to framework remote 802.11 systems. To complete such assaults just ware equipment and programming parts are required. The outcomes demonstrate that genuine vulnerabilities exist in various access focuses and that a solitary noxious station can without much of a stretch frustrate any authentic correspondence inside an essential administration set.

#3 Detecting Identity Based Attacks in Wireless Networks Using Signal prints

Remote systems are powerless against numerous character based assaults in which a noxious gadget utilizes manufactured MAC delivers to take on the appearance of a particular customer or to make different ill-conceived personalities. For instance, a few connection layer benefits in IEEE 802.11 systems have been appeared to be powerless against such assaults notwithstanding when 802.11i/1X and other security components are sent.

In this paper we demonstrate that a transmitting gadget can be heartily recognized by its flag print, a tuple of flag quality esteems revealed by get to focuses going about as sensors. We demonstrate that, not quite the same as MAC addresses or other bundle substance, assailants don't have as much control in regards to the signalprints they deliver .Moreover, utilizing estimations in a testbed arrange, we exhibit that signalprints are emphatically associated with the physical area of customers, with comparable esteems discovered for the most part in nearness. By labeling suspicious bundles with their relating signalprints, the system can heartily recognize every transmitter autonomously of parcel substance, permitting location of a huge class of character based assaults with high likelihood.

#4 Secure and Efficient Key Management in Mobile Ad Hoc Networks

In portable impromptu systems, because of inconsistent remote media, have portability and absence of foundation, giving secure interchanges is a major test in this one of a kind system condition. Normally cryptography systems are utilized for secure correspondences in wired and remote systems. The unbalanced cryptography is broadly utilized on account of its adaptability (validation, trustworthiness, and classification) and effortlessness for key conveyance. Be that as it may, this approach depends on a brought together system of open key framework (PKI). The symmetric approach has calculation proficiency, yet it experiences potential assaults on key understanding or key conveyance. Truth be told, any cryptographic means is insufficient if the key administration is powerless. Key administration is a focal angle for security in versatile specially appointed systems. In versatile specially appointed systems, the computational load and intricacy for key administration is firmly subject to confinement of the hub's accessible assets and the dynamic idea of system topology.

In this paper, we propose a protected and proficient key administration structure (SEKM) for versatile specially appointed systems. SEKM assembles PKI by applying a mystery sharing plan and a hidden multicast server gathering. In SEKM, the server bunch makes a perspective of the accreditation specialist (CA) and gives endorsement refresh administration to all hubs, including the servers themselves. A ticket plot is presented for effective authentication benefit. Also, a productive server gather refreshing plan is proposed.

#5 Spatial Signatures for Lightweight Security in Wireless Sensor Networks

This paper tentatively explores the practicality of without crypto correspondences in asset compelled remote sensor systems. We misuse the spatial mark actuated by the radio correspondences of a hub on its neighboring hubs. We outline a primitive that heartily and productively understands this idea, even at the level of individual parcels and when the system is generally inadequate. Utilizing this primitive, we outline a convention that powerfully and effectively approves the genuineness of the wellspring of messages: bona fide messages cause no correspondence overhead though disguised interchanges are distinguished helpfully by the neighboring hubs. The convention empowers lightweight intrigue safe strategies for communicate verification, unicast validation, non-renouncement and respectability of correspondence. We have actualized our primitive and convention, and evaluated the abnormal state of exactness of the convention by means of

Testbed experiments with *CC1000* radio-enabled motes and *802.15.4* radio-enabled motes.

3. IMPLEMENTATION

1. Node Configuration

a. Link Configuration

In this module Nodes are configured based on number of nodes in need of packet requisition. We create the network group by connecting nodes to sink. Link configuration means connecting the nodes and intermediate nodes to the sink.

2. Sender Node

a. Packet Splitting

In this module, Sender selects the file which is to be sent. And then it split into the number of packets based on the size for adding some bits in it.

b. Send Packets to Intermediate

And then it encrypts all the splitted packets. And then sender adds some bits to each encrypted packets before sending that. Bit Addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node.

3. Intermediate Node(Router)

a. Send Packets to Sink

In this module, the intermediate node receives Packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication. Before sending to sink, intermediate add some bits to each packet for node identification. After adding some bits from intermediate, it sends all packets to the sink.

b. Modify or Drop

Before sending all packets to sink, packets dropping or packets modifying may be occur in intermediate.

4. Sink

a. Verify

In this module, Sink receives all packets from the sender node, and it verifies all packets which are dropped or not. And it also verifies the packets which are modified or not and it can identify the modifiers in the process based on the bit identification.

b. Merge Packets

After receiving all packets in sink, it decrypts all packets. After the decryption if there is no modified or dropped packets, it merge all packets. After merging, Sink can receive the original file.

c. Categorization And Ranking

In this module Categorization and Ranking will be performed based on the node behavior. If there is any modification or drop of packets in node it assumes negative value for modifier or dropper. Sink performs Ranking for each node based on the Category of nodes. Sink gives ranking like Good, Temporarily Good, Suspiciously Bad, Bad based on the node behavior in the process

4. RELATED WORK

A. Network Model: We have make a multihop remote sensor organize, comprising of various sensor hub and a base station that gathers information from the system. The systems is demonstrated as a diagram G(N, L), where N = {n I |, 1 ≤ I ≤ |N |} is the arrangement of hubs, and L is the arrangement of connection, containing a component l i,j for each match ofnodes n I and n j that are discussing straightforwardly with each other. The Base station relegates every hub a remarkable identifier nodeID and a symmetric cryptographic key K I .

B. Data Model: We consider a numerous round procedure of gathering information. Every sensor produces information intermittently, and singular esteems areaggregated towards the Base station utilizing any current various leveled dispersal conspire . Every datum parcel contains of (I) a one of a kind bundle arrangement number, (ii) an information esteem, and (iii) provenance.

C. Threat Model: It is additionally essential to give Data-Provenance Binding i.e., a coupling amongst information and provenance so anattacker can't effectively drop or change the genuine information while holding the provenance, or swap the provenance of two parcels.

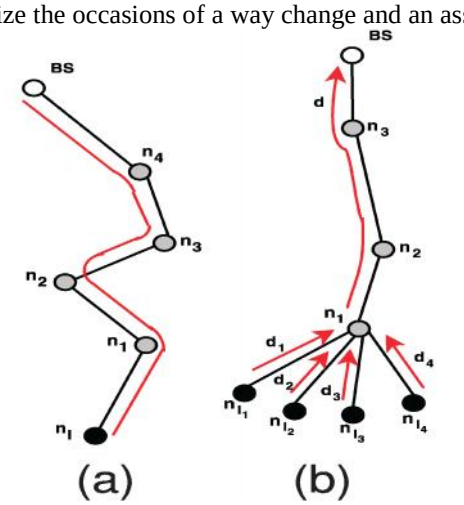
D. The Bloom Filter (BF): A few BF varieties that give extra usefulness exist. A Counting Bloom Filter (CBF) partners a little counter with each piece, which is

augmented/decremented upon thing inclusion/erasure. To answer rough set participation inquiries, the separation touchy Bloom channel has been proposed. In any case, collection is the main operation required in our concern setting. The combined idea of the fundamental BF development characteristically bolsters the conglomeration of BFs of a same kind, so we don't require CBFs or other BF variations.

E.Provenance Decoding: At the point when a Base station gets an information parcel .Base station comprehend what the information bundle ought to be checks. A while later, after accepting a bundle, it is adequate for the BS to confirm its information of provenance with that encoded in the packet. **Algorithm-1 Provenance Verification:**

Input: Received packet with sequence seq and iBF ibf.
Set of hash functions H, Data path P = < n l 1 , ..., n 1 , ..., n p >
BF c ← 0 // Initialize Bloom Filter
for each n i P do
vid i = generateVID (n i , seq)
insert vid i into BF c using hash functions in H endfor
if (BF c = ibf) then
return true // Provenance is verified
endif return false.

Algorithm 1 demonstrates the means to confirm provenance for a given bundle. We expect that the information of the BS about this current parcel's way is P_. At in the first place, the BS instates a Bloom channel BFc with every one of the 0's. The BF is then refreshed by producing the VID for every hub in the way P_ and embeddings this ID into the BF. BFc now mirrors the view of BS about the encoded provenance. To approve its discernment, the BS at that point thinks about BFc to the got ibf . The provenance confirmation succeeds just if BFc is equivalent to ibf . Something else, if BFc varies from the got iBF, it demonstrates either an adjustment in the information stream way or a BF alteration assault. The check disappointment triggers the provenance gathering process which endeavors to recover the hubs from the encoded provenance and furthermore to recognize the occasions of a way change and an assault.



Provenance graph for a sensor network

5. CONCLUSION

In this paper, proposed the issue of safely transmitting provenance for sensor organizes, and proposed a light-weight provenance encoding and translating plan in light of Bloom channels. The plan guarantees classification, honesty and freshness of provenance. We stretched out the plan to consolidate information provenance official, and to incorporate bundle succession data that backings recognition of parcel misfortune assaults. Exploratory and diagnostic assessment comes about demonstrate that the proposed plot is compelling, light-weight and versatile. In future work, we intend to actualize a genuine framework model of our protected provenance plot, and to enhance the precision of parcel misfortune identification, particularly on account of numerous successive malevolent sensor hubs.

REFERENCES

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in *Proc. of Data Management for Sensor Networks*, 2010, pp. 2–7.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A virtual data system for representing, querying, and automating data derivation," in *Proc. of the Conf. on Scientific and Statistical Database Management*, 2002, pp. 37–46.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in *Proc. of the USENIX AnnualTechnical Conf.*, 2006, pp. 4–4.

[4] Y. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," *SIGMOD Record*, vol. 34, pp. 31–36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in *Proc. Of FAST*, 2009, pp. 1–14.

[6] S. Madden, J. Franklin, J. Hellerstin, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," *SIGOPS Operating Systems Review*, no. SI, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An efficient clustering based heuristic for data gathering and aggregation in sensor networks," in *Proc. of Wireless Communications and Networking Conference*, 2003, pp. 1948–1953.

[8] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in *Proc. of ICDCS Workshops*, 2011, pp. 332–338.

[9] L. Fan, P. Cao, J. Almeida, and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol," *IEEE/ACM Trans. Netw.*, vol. 8, no. 3, pp. 281–293, Jun. 2000.

[10] A. Kirsch and M. Mitzenmacher, "Distnce-sensitive bloom filters," in *Proc. of the Workshop on Algorithm Engineering and Experiments*, 2006, pp. 41–50.

[11] C. Rothenberg, C. Macapuna, M. Magalhaes, F. V rdi, and A. Wiesmaier, "In-packet bloom filters: Design and networking applications," *Computer Networks*, vol. 55, no. 6, pp. 1364 – 1378, 2011.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-netwok aggregation," in *ICDE*, 2007, pp. 84–89.

[13] T. Wolf, "Data path credentials for high-performance capabilitiesbased networks." in *Proc. of ACM/IEEE Symp. on Architectures for Networking and Communications Systems.*, 2008, pp. 129–130.

[14] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. of the conf. on Computer and communications security (CCS)*, 2006, pp. 278–287.

[15] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1040–1052, 2012.