Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 2, February -2017

Conserving and Detecting Packet Dropping Attacks in Wireless Networks Using Bloom Filter

[1]Chandraveer Kumar, [2]Shubham Chidrewar, [3]Satish Kumar, [4]Prof. Gargi Joshi,

Dept.Of.IT. Dr. D. Y. Patil Educational Academys
DEPARTMENT OF INFORMATION TECHNOLOGY,Ambi,Pune

Abstract--- *Large-scale ad-hoc systems are deployed in various application areas and the data they gather are utilized as a part of decision-making for critical infrastructures. Data are streamed from different sources through intermediate processing nodes that aggregate information. A malicious adversary may present extra nodes in the network or compromise existing ones. Therefore, guaranteeing high data trustworthiness is crucial for right decision-making. In this paper, we propose a novel Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks to securely transmit sensor data. The proposed method depends on in packet Bloom filters to encode the data. We present productive mechanisms for data verification and reconstruction at the base station. In addition, we expand the protected data scheme with functionality to detect packet drop organized by malicious data sending nodes. We assess the proposed system both analytically and experimentally, and the outcomes demonstrate the adequacy and efficiency of the Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks in detecting packet forgery and los attacks.*

Keywords--- *Bloom Filters, Publish/Subscribe Multicast, Forwarding, Security, Sensor Networks.*

I. INTRODUCTION

Sensor networks have become ever more popular in in several application domains, like cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data are built at many sensor node sources and processed in-network at intermediate hops on their way to some base station that performs decision-making. The range of information sources creates the necessity to assure the trustworthiness of data, so that only trustworthy details are considered within the decision process. Data is an efficient approach to assess data trustworthiness, since it summarizes a brief history of ownership as well as the actions performed on the data. Recent research highlighted the key contribution of information in systems where the usage of untrustworthy data can lead to catastrophic failures e.g. SCADA systems for critical infrastructure. Although data modeling, collection, and querying have already been investigated extensively for workflows and curated databases, data in sensor networks hasn't been properly addressed. In this paper, we investigate the problem of safe and efficient data transmission and processing for sensor networks. In a multi-hop sensor network, data enables the base station to trace the origin and forwarding path of an individual data packet since its generation. Data must be recorded for each and every data packet, but important challenges arise due to tight storage, energy and bandwidth constraints of the sensor nodes. Therefore, it is necessary to devise a light-weight data solution which doesn't introduce significant overhead. Furthermore, sensors often operate in an untrusted environment, where they might be subject to attacks. Hence, it is necessary to report security requirements alike confidentiality, integrity and freshness of provenance the system.

II. LITERATURE SURVEY

2.1 Paper Name: ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks
Authors: B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens
Description: Ad hoc networks provide multiplied coverage by exploitation multi-hop communication. This design makes services a lot of liable to internal attacks coming back from compromised nodes that behave arbitrarily to disrupt the network, additionally observed as Byzantine attacks. During this work, we examine the impact of many Byzantine attacks performed by individual or colluding attackers. We propose ODSBR, the primary on-demand routing protocol for unintended wireless networks that gives resilience to Byzantine attacks caused by individual or colluding nodes. The protocol uses an adaptive probing technique that detects a malicious link once log n faults have occurred, where n is the length of the trail. Problematic links are avoided by employing a route discovery mechanism that relies on a brand new

metric that captures adversarial behavior. Our protocol ne'er partitions the network and bounds the number of harm caused by attackers. We have a tendency to demonstrate through simulations ODSBR's effectiveness in mitigating Byzantine attacks. Our analysis of the impact of those attacks versus the adversary's effort provides insights into their relative strengths, their interaction, and their importance once planning multi-hop wireless routing protocols.

2.2 Paper Name: TWOACK: Preventing selfishness in mobile ad hoc networks
Authors: K. Balakrishnan, J. Deng, and P. K. Varshney,
Description: Mobile spontaneous Networks (MANETs) operate the basic underlying assumption that each one taking part nodes totally collaborate in self-organizing functions. However, performing network functions consumes energy and different resources. Therefore, some network nodes might decide against cooperating with others. Providing these egotistic nodes, conjointly termed misbehaving nodes, with associate incentive to collaborate has been a vigorous analysis area recently. During this paper, authors tend to propose 2 network-layer acknowledgment-based schemes, termed the TWOACK and also the S-TWOACK schemes, which may be merely added-on to any source routing protocol. The TWOACK theme detects such misbehaving nodes, and then seeks to alleviate the matter by notifying the routing protocol to avoid them in future routes. Details of the 2 schemes and our analysis results supported simulations square measure given during this paper. We've found that, in a network wherever up to four-hundredth of the nodes is also misbehaving, the TWOACK theme ends up in two hundredth improvement in packet delivery magnitude relation, with an inexpensive further routing overhead.

2.3 Paper Name: Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited
Authors: R. Rao and G. Kesidis
Description: Ad hoc networks square measure gaining presence with the proliferation of low-cost wireless devices and also the got to keep them connected. Individual applications and bigger missions, like those of military science sensing element networks, require secure knowledge transmission among wireless devices. Security remains a serious challenge for such networks. Current protocols use coding and authentication techniques for secure message exchange, however given the limitations and innately insecure nature of ad-hoc networks, such mechanisms might not serve. A security breach can, as an example, be a network-level denial-of-service (DoS) attack, passive eavesdropping, or physical layer jam to degrade communication channels. In a multihop network, associate degree entrant node will degrade communication quality by merely dropping packets that are meant to be relayed (forwarded). The network might then misinterpret the reason for packet loss as congestion instead of malicious activity. During this paper, we suggest that traffic transmission patterns be designated to facilitate verification by a receiver. Such traffic patterns square measure used in concert with suboptimal mackintosh that preserves the statistical regularity from hop to hop. This general technique for intrusion detection is so appropriate for networks that don't seem to be information measure restricted however have strict security necessities, e.g., bound styles of military science sensor networks.

2.4 Paper Name: Secure data collection in wireless sensor networks using randomized dispersive routes
Authors: T. Shu, M. Krunz, and S. Liu
Description: Compromised-node and denial-of-service square measure 2 key attacks in wireless sensing element networks (WSNs). During this paper, we study routing mechanisms that circumvent (bypass) black holes formed by these attacks. We have a tendency to argue that existing multi-path routing approaches square measure susceptible to such attacks, chiefly because of their deterministic nature. Thus once associate degree someone acquires the routing algorithm, it will reckon constant routes best-known to the supply, and therefore endanger all data sent over these routes. In this paper, we have a tendency to develop mechanisms that generate randomized multipath routes. Below our style, the routes taken by the "shares" of different packets modification over time. Thus notwithstanding the routing algorithm becomes best-known to the someone, the someone still cannot pinpoint the routes traversed by every packet. Besides randomness, the routes generated by our mechanisms also are highly dispersive and energy-efficient, creating them quite capable of bypassing black holes at low energy price. In depth simulations are conducted to verify the validity of our mechanisms.

2.5 Paper Name: The feasibility of launching and detecting jamming attacks in wireless networks
Authors: W. Xu, W. Trappe, Y. Zhang, and T. Wood
Description: Wireless networks are engineered upon a shared medium that makes it simple for adversaries to launch jamming-style attacks. These attacks will be simply accomplished by a person emitting frequency signals that don't

follow an underlying raincoat protocol. Electronic countermeasures attacks will severely interfere with the conventional operation of wireless networks and, consequently, mechanisms are required which will deal with jamming attacks. During this paper, we have a tendency to examine radio interference attacks from either side of the issue: 1st, we have a tendency to study the problem of conducting radio interference attacks on wireless Networks, and second we have a tendency to examine the crucial issue of diagnosis the presence of electronic countermeasures attacks. Specifically, we propose four totally different electronic countermeasures attack models which will be used by a person to disable the operation of a wireless network, and judge their effectiveness in terms of however each methodology affects the power of a wireless node to send and receive packets. We have a tendency to then discuss totally different measurements that function the idea for police investigation an electronic countermeasures attack, and explore eventualities wherever every measuring by itself isn't enough to dependably classify the presence of an electronic countermeasures attack. In explicit, we have a tendency to observe that signal strength and carrier sensing time are unable to once and for all sight the presence of a transmitter. Further, we have a tendency to observe that though by using packet delivery magnitude relation we have a tendency to could differentiate between full and crowded eventualities, we have a tendency to are still unable to conclude whether or not poor link utility is thanks to electronic countermeasures or the mobility of nodes. the actual fact that no single measuring is sufficient for dependably classifying the presence of a transmitter is an important observation, and necessitates the event of increased detection schemes which will take away ambiguity when police investigation a transmitter. To handle this would like, we propose two increased detection protocols that use consistency checking. the primary theme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, whereas the second theme employs location information to function the consistency check. Throughout our discussions, we have a tendency to examine the practicability and effectiveness of electronic countermeasures attacks and detection schemes victimization the MICA2 Mote platform.

III. EXISTING SYSTEM

Existing root kit detection work includes characteristic suspicious call execution patterns, discovering vulnerable kernel hooks, exploring kernel in variants, or employing a virtual machine to enforce correct system behaviors. In existing your time suspicious information not detected.

Recent analysis highlighted the key contribution of information in systems wherever the utilization of undependable data might cause ruinous failures (e.g., SCADA systems). Though information modeling, collection, and querying are studied extensively for workflows and curated databases, information in sensing element networks has not been properly addressed

3.1 Disadvantages of Existing System:

1. Traditional data information security solutions use intensively cryptography and digital signatures, and that they use append-based information structures to store cradle, resulting in preventive prices.
2. Existing analysis employs separate transmission channels for information and cradle.
3. In existing your time suspicious information not detected.

IV. PROPOSED SYSTEM

We're designing an information encoding and decoding mechanism that satisfies security and performance needs. We advise a knowledge encoding strategy whereby each node on the way of your data packet securely embeds data information inside a Bloom filter (BF) that is transmitted combined with the data. Upon receiving the packet, the BS extracts and verifies the info information. In addition we devise an extension cord of the data encoding scheme which allows the BS to identify if the packet drop attack was staged by the malicious node.

We use only fast message authentication code (MAC) schemes and Bloom filters that happen to be fixed-size data structures that compactly represent provenance. Bloom filters make efficient using of bandwidth, and they yield low error rates utilized. We formulate the problem of secure data transmission in sensor networks, and find out the challenges specific to this context. We propose an in-packet Bloom filter (iBF) data -encoding scheme.

4.1 Advantages of Proposed System:

1. Our design is efficient approaches for data decoding and verification with the base station.

2. We extend the secure data encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
3. We execute a detailed security analysis and satisfaction look at the proposed data encoding scheme and packet loss detection mechanism.
4. We only have to have a single channel for both transmission channels for data and provenance.

V. SYSTEM ARCHITECTURE

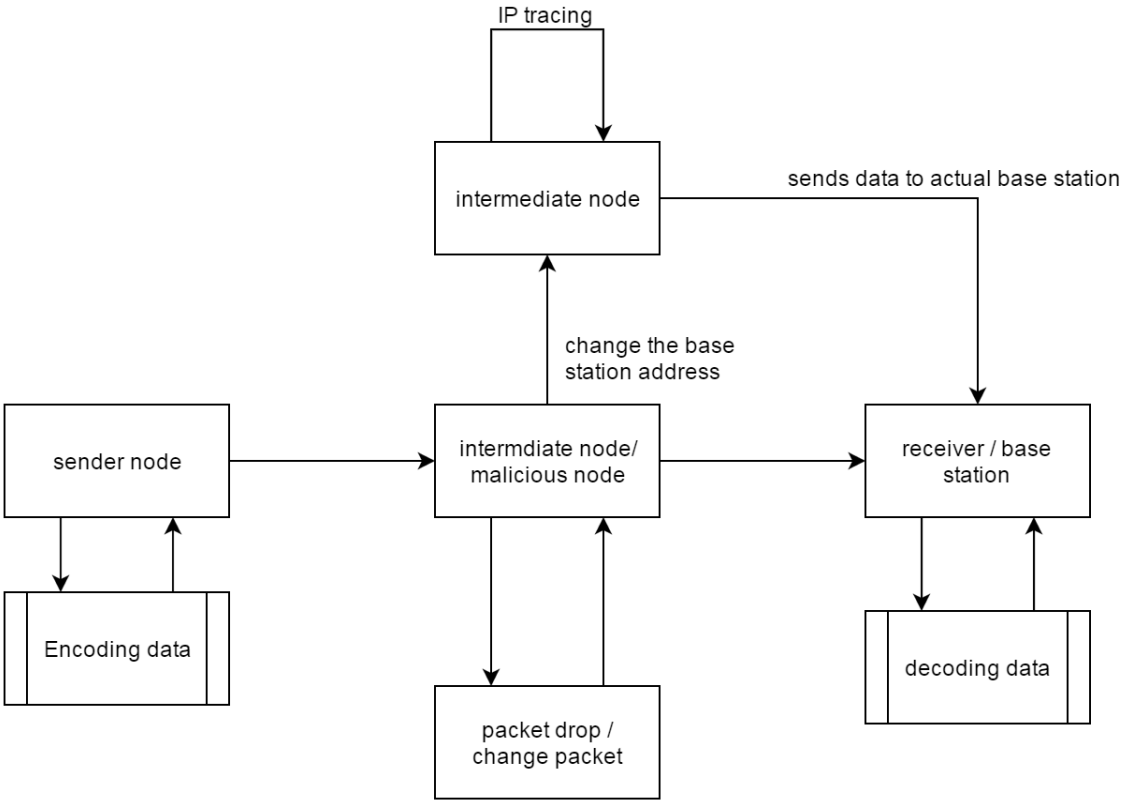

Figure 1. System Architecture of Proposed System

VI. MATHEMATICAL MODEL

Let W be the whole system which consists:
W= {IP, PRO, OP}
IP is the input of system.
IP= {BS, G, N, L, K, H, d, ID, V, E, S, BF}.
Where,

1. Let BS is the Base Station which collects data from network.

2. Let G is the graph , G(N,L)
   Where, N is the set of nodes.

   $N = \{ni|, 1 \leq i \leq |N|\}$ is the set of nodes,
   And L is the set of links, containing an element li,j for each pair of nodes ni and nj that are communicating directly with each other.

3. K is set of symmetric cryptographic key

4. H is a set of hash functions

   H = {h1, h2, ..., hk} .

5. E is edge set consists of directed edges that connect sensor nodes.

6. d is the set of data packets,

Let G is acyclic graph G (V,E) where each vertex v ∈ V is attributed to a specific node HOST(v) = n and represents the data record (i.e. nodeID) for that node.
Each vertex in the graph is uniquely identified by a vertex ID (VID) which is generated by the host node using cryptographic hash functions.

Procedure:
Let S is a set of items
S = {s1, s2, ..., sn}
We use an array of m bits with k independent hash functions h1, h2, ..., hk.
The output of each hash function hi maps an item s uniformly to the range [0, m-1], i.e., an index in a m-bit array.
Let BF is the Bloom Filer, can be represented as {b0, . . . , bm−1}.
Initially all m bits are set to 0.
To insert an element s ∈ S into a BF, s is hashed with all the k hash functions producing the values hi(s) ($1 \leq i \leq k$).
The bits corresponding to these values are then set to 1 in the bit array.
To query the membership of an item s` within S, the bits at indices hi(s`) ($1 \leq i \leq k$) are checked. If any of them is 0, then certainly s` not within S. Otherwise, if all of the bits are set to 1, s`∈ S with high probability.

There exists a possibility of error which arises due to hashing collision that makes the elements in S collectively causing indices hi(s`) being set to 1 even if s` not within S. This is called a false positive.

VII. CONCLUSION

We addressed the situation of securely transmitting data for sensor networks, and proposed a data encoding and decoding scheme determined by Bloom filters. The scheme ensures confidentiality, integrity and freshness of information. We extended the scheme to incorporate data binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme works, light-weight and scalable. Later on work, we want to implement a real system prototype individual's secure scheme, and also to increase the accuracy of packet loss detection, especially in the matter of multiple consecutive malicious sensor nodes.

REFERENCES

[1] Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet dropping Attacks in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 4, APRIL 2015

[2] W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.

[4] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[5] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610.

[6] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[7] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[8] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[9] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," in Proc. IEEE GLOBECOM Conf., 2003, pp. 2957–2961.

[10] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM MobiHoc Conf., 2005, pp. 46–57.

