NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 7, July-2017

PACKET DROP ATTACK DETECTION AND PRIVACY MANAGEMENT FOR CONFIDENTIAL MULTIHOP COMMUNICATION IN WIRELESS NETWORK

MR.MATHAPATI RAJSHEKHAR
ME. Student, Dept. Of Comp. Engg. Flora Institute Of Technology, Pune, Maharashtra, India,
mathapati.rajshekhar@gmail.com

ASST. PROF. JOSHI SHWETA
Asst. Prof. Dept. Of Comp. Engg. Flora Institute of Technology, Pune, Maharashtra, India, shweta.kshirsagar@gmail.com

ABSTRACT:

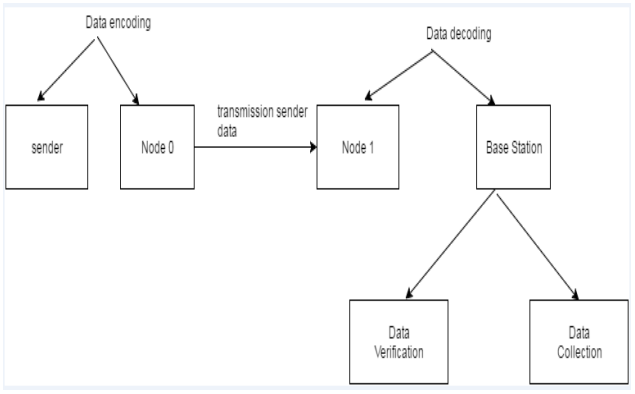
Sensor networks are becoming additional and additional widespread in varied application domains, like cyber physical infrastructure systems, environmental looking, power grids, etc. information area unit created at Associate in nursing outsized sort of device node sources and processed in-network at intermediate hops on their due to a base station that performs decision-making. The range of data sources creates the need to assure the attribute of data, such entirely trustworthy data is taken under consideration among the decision methodology. Information is associate in nursing economical methodology to assess info attribute, since it summarizes the history of possession and thus the actions performed on the data. We tend to tend to tend to propose a really distinctive Truthful Detection of Packet Dropping Attacks in Wireless spontaneous Networks to firmly transmit device info. The planned technique depends on in packet Bloom filters to inscribe the information. We tend to productive mechanisms for information verification and reconstruction at very cheap station. To boot, we tend to expand the protected info theme with utility to observe packet drop organized by malicious info exploit nodes. We tend to tend to tend to assess the planned system each analytically and through an experiment, so the outcomes demonstrate the adequacy and potency of the Truthful Detection of Packet Dropping Attacks in Wireless spontaneous Networks in detection packet forgery and d-dos attacks.

KEYWORDS: Attack-tolerant, Sensor Network, Bloom Filter, WSN, MAC.

I. INTRODUCTION:

In a multi-hop device network, knowledge source permits the bottom station to trace the supply and forwarding path of a personal knowledge packet since its generation. Source should be recorded for every knowledge packet; however vital challenges arise as a result of the tight storage, energy and information measure constraints of the device nodes. Therefore, it's necessary to plot a light-weight source resolution that doesn't introduce important overhead. What is more, sensors typically operate in associate degree untrusted atmosphere, wherever they'll be subject to attacks. Hence, it's necessary to handle security needs like confidentiality, integrity and freshness of source. Our goal is to style a source encryption and decipherment mechanism that satisfies such security and performance wants. We have a tendency to propose a source encryption strategy whereby every node on the trail of an information packet firmly embeds source information among a Bloom filter that is transmitted together with the information. Upon receiving the information, the bottom station extracts and verifies the source.

Data source is a good methodology to assess knowledge trustiness, since it summarizes the history of possession and therefore the actions performed on the information. Recent analysis highlighted the key contribution of source in systems wherever the employment of unreliable knowledge might cause ruinous failures e.g. SCADA systems for essential infrastructure. Though source modeling, collection, and querying are investigated extensively for workflows and curated databases, source in device networks has not been properly self-addressed. During this paper, we have a tendency to investigate the matter of secure and economical source transmission and process for device networks.



II. LITERATURE REVIEW:

2.1 PAPER NAME: Secure Data Aggregation in Wireless Sensor Networks

AUTHORS: Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia.
DESCRIPTION: The paper discuss the security issues of in-network aggregation algorithms to compute aggregates such as establish Count and Sum also discussed how a cooperated node can corrupt the aggregate estimation of the base station, keeping our effort on the ring-based hierarchical aggregation algorithms. To address this problem, obtainable a lightweight confirmation algorithm which would enable the base station (BS) to confirm whether the computed aggregate was valid.

2.2 PAPER NAME: Resource allocation and cross-layer control in wireless networks
AUTHORS: Georgiadis, Leonidas, Michael J. Neely, and Leandros Tassiulas.
DESCRIPTION: In this paper author presents abstract models that capture the cross-layer interaction from the physical to move layer in wireless network architectures as well as cellular, ad-hoc and device networks likewise as hybrid wireless-wire line.

2.3 PAPER NAME: A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks.
AUTHORS: Salmin Sultana, Gabriel Ghinita, Elisa Bertino, Fellow, and Mohamed Shehab.
DESCRIPTION: A mischievous adversary may familiarize further nodes in the network or cooperation existing ones. Therefore, assuring high information trustworthiness is crucial for right decision-making. Planned a novel lightweight system to strongly transmit provenance for sensor files.

2.4 PAPER NAME: In-packet Bloom filters: Design and networking applications
AUTHORS: Christian E. Rothenberg, Carlos A. B. M., Maur´ıcio F. Magalhaesa, F´abio L. V., A. Wiesmaierc.
DESCRIPTION: This paper explores an exciting front in the Bloom filter research space, namely the special category of small Bloom filters carried in packet headers. Using iBFs is a promising approach for networking application designers choosing to move application state to the packets themselves. At the expense of some false positives, fixed-size iBFs are amenable to hardware and present a way for new networking applications.

2.5 PAPER NAME: On the connection-level stability Of congestion controlled communication networks
AUTHORS: Lin, Xiaojun, Ness B. Shroff, and R. Srikant.
DESCRIPTION: In this paper, this time-scale separation assumption is removed and it is shown that the largest possible stability region can still be achieved by a large class of control algorithms.

III. DEVELOPED 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) systems and Bloom filters that occur 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 frame the problem of secure data transmission in sensor networks, & find obtainable the challenges specific to this context. We propose an in-packet Bloom filter (iBF) data -encoding scheme.

3.1 ADVANTAGES OF DEVELOPED SYSTEM:

1. To achieve confidentiality, one needs to encode blocks of information across multiple packets. Developed a novel adaptive end-to-end encoding scheme, that takes certain observations from the network and chooses the appropriate code rate to maintain confidentiality for each block of data.
2. The system can efficiently detect the actual packet loss in the wireless network.
3. In secure confidetional wireless communications between Multihop networks.

IV. SYSTEM ARCHITETURE:

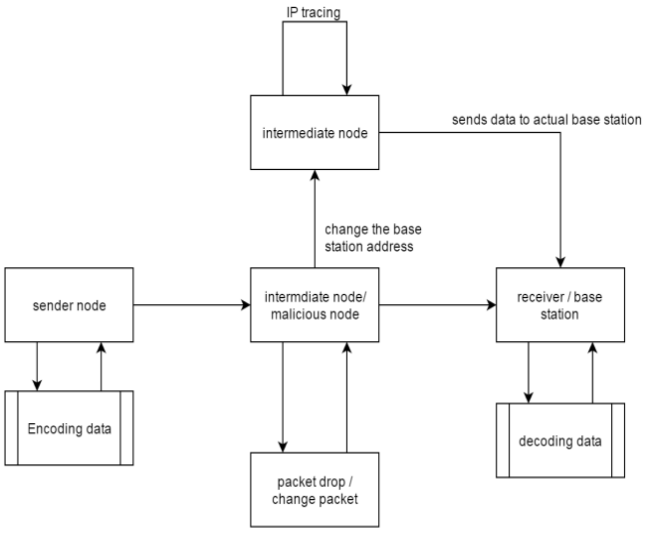


Figure 4.1 System Architecture of Developed System

4.1 WORKING OF DEVELOPED SYSTEM:

1. Source node sends messages toward the destination node.
2. Message devides in number of packets and encoded.
3. At intermediate node packet receives packets, it can change or drop packets by various any hackers. Intermediate node can change destination address. If it changes address, then it can trace by IP tracing.
4. At destination node when it receives packets then decoding of message is happen.

4.2 SYSTEM FEATURES:

1. PRIVACY MANAGEMENT:

In this project, privacy management is achieved by introducing the bloom filter mechanism, the system will assign the unique sequence to each package when it sending from sender. After reaching that packets at destination side the destination node will applies the bloom filter mechanism to verify the packets.

2. PARALLEL COMPUTING:

This developed system will come under parallel computing because the sender node will send the message to destination node but at the backend system will encode that message data i.e. dividing into multiple packets and assigning the sequence number to that message which is required to filter and detect the packet drop attack. And also system will continuously send status report to sender about packet drop.

3. DISTRIBUTED DATABASE:

When sender is sending the message to destination, then at the back end system will divide that data into multiple packages (we are considering 3) i.e. message is divided into 3 different packages while sending and each intermediate node in the network will receive the message in 3 different packages.

4. INTRUSION DETECTION:

In intrusion detection, we are detecting the packet drops attacks and IP tracing. Packet drop attack means the intermediate node or mediator node or attacker node will drop the while forwarding to next node and IP tracing means when attacker changes the destination IP address of node then system will trace that actual destination IP and forward the message to that IP address.

5. VERIFY DATA INTEGRITY:

Data integrity is maintained by MD5. If intruder changes the packet data, with the help of MD5 we can detect any changes in data. By using MD5 hash value is generated at sender or source side and at the receiver side also. So by comparing hash values at both the sides, integrity of data is verified.

V. 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, $1 \le i \le |N|$} is the set of nodes,
   And L is the set of links, containing an element li,jfor each pair of nodes niand njthat 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 setconsists 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 $v \in V$ 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 suniformly to the range [0, m-1], i.e., an index in am-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 $s \in S$ into a BF, s is hashed with all the k hash functions producing the values hi(s) ($1 \le i \le k$).

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`) ($1 \le i \le k$) are checked. If any of them is 0, then certainly s` not within S. Otherwise, if all of the bits are set to 1, $s` \in S$ 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.

VI. RESULT ANALYSIS:

6. 1 COMPARISON WITH EXISTING SYSTEM:

	Existing System	Developed System
P	50	85
Q	55	79
R	75	55

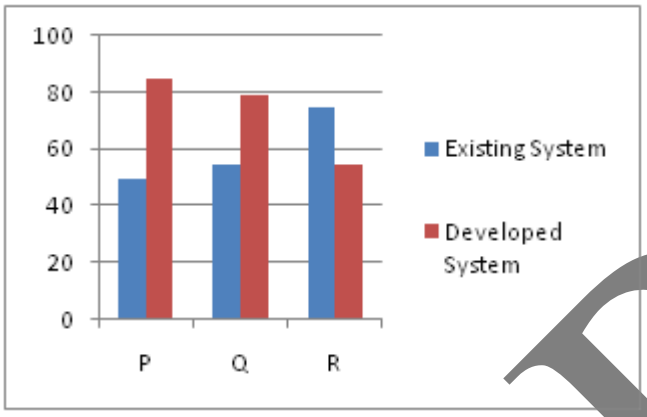


Figure 4.2 Comparisons with Existing System

Where, P – Confidentiality, Q – Performance, R – Delay Rate

6.2 INPUT:

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the Time and performance of system. Considering few attributes like detection accuracy, confidentiality and time predicted analytical results of developed system with respect to existing system.

RESULT:

	Existing System	Developed System
A	3	10
B	6	10
C	8	4

Where,
A = Detection Accuracy.
B = Confidentiality.
C = Time.

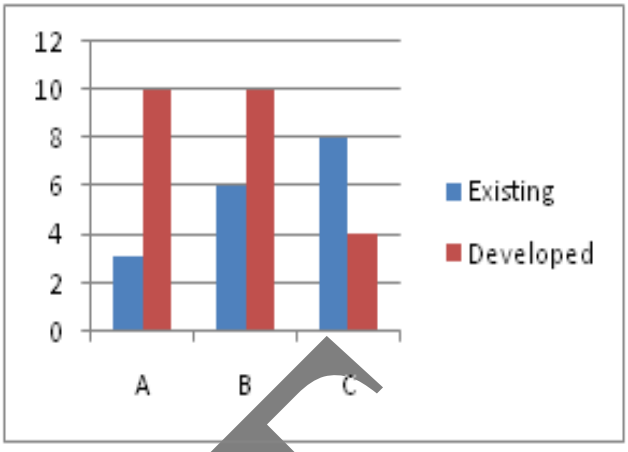


Figure 4.3 Final Result with Graph

VII. CONCLUSION AND FUTURE SCOPE:

In this paper, we considered the problem of packet drop attack detection in wireless multi-hop networks where sources have confidential information to be transmitted to their corresponding destinations with the help of intermediate nodes where there is no trust over the intermediate nodes. All intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. To provide confidentiality in such setting, developed encoding and decoding the message over blocks of information which are transmitted over different path of communication. 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) Sultana, Salmin, et al. *"A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks*." IEEE Transactions on dependable and secure computing 12.3 (2015): 256-269.
2) Roy, Sankardas, et al. "*Secure data aggregation in wireless sensor networks."* IEEE Transactions on Information Forensics and Security 7.3 (2012): 1040-1052.
3) Rothenberg, Christian Esteve, et al. "*In-packet Bloom filters: Design and networking applications.*" Computer Networks 55.6 (2011): 1364-1378.
4) Lim, Hyo-Sang, Yang-Sae Moon, and Elisa Bertino. *"Provenance-based trustworthiness assessment in sensor networks*." Proceedings of the Seventh International Workshop on Data Management for Sensor Networks.ACM, 2010.
5) 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.

6) 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.
7) 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.
8) Lin, Xiaojun, Ness B. Shroff, and R. Srikant. "*On the connection-level stability of congestion-controlled communication networks."* IEEE Transactions on Information Theory 54.5 (2008): 2317-2338.
9) Georgiadis, Leonidas, Michael J. Neely, and Leandros Tassiulas. "*Resource allocation and cross-layer control in wireless networks*." Foundations and Trends® in Networking 1.1 (2006): 1-144.