Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 5, May-2017

"Security on MANET Using Block Coding"

[1]Gajanan Murkute, [2]Sanjay Nangare, [3]Vishwambar Sable, [4]Prof.C.G.Thorat

Department of Computer Engineering, Rajarshi Shahu College of Engineering, Pune,India

***Abstract* — Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this paper, we propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in packet Bloom filters to encode provenance.**

Keywords- MANET, Dynamic Network Topology, Security Block.

I. INTRODUCTION

Sensor networks are becoming increasingly popular in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. Recent research highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures e.g. SCADA systems for critical infrastructure. Although provenance modeling, collection, and querying have been investigated extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed.

II. PROBLEM STATEMENT

Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this project, we are proposing a novel lightweight scheme to securely transmit provenance for sensor data. If both level of security is right, then client will give apportion as indicated by smart card. Apportion will disperse utilizing dc motor and after circulation through IOT innovation message will send to approve individual. Individual will see that message on Mobile/PC in graphical way utilizing web. If any level fizzles, buzzer will ready as sign and picture of brilliant card will send to approve individual PC/Mobile.

III. LITERATURE REVIEW

SR.NO	PAPER NAME	AUTHORS	DESCRIPTION
1.	A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks.	Salmin Sultana,Gabriel Ghinita, Elisa Bertino, Fellow, and Mohamed Shehab	A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Proposed a novel lightweight scheme to securely transmit provenance for sensor data.

2.	In-packet Bloom filters: Design and networking applications	Mohit Agarwal1, Manish Sharma2, Bhupendra Singh3, Shantanu	In this framework, a RFID tag is utilized that conveys the relative subtle elements .The microcontroller associated with the reader will checks for the client validation. On the off chance that the client is discovered true then the amount of proportion to be given to the client &will be shown in plain view device.
3.	Secure Data Aggregation in Wireless Sensor Networks	Christian E. Rothenberg, Carlos A. B. M., Maur´ıcio F. Magalhaesa, F´abio L. V., A. Wiesmaierc	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.
4.	Provenance based Trustworthiness Assessment in Sensor Networks	Hyo Sang Lim, Yang Sae Moon, South Korea Elisa Bertino	Proposed a systematic method for assessing the trustworthiness of data items. This approach uses the data provenance as well as their values in computing trust scores, that is, quantitative measures of trustworthiness. To obtain trust scores, proposed a cyclic framework which well reflects the inter-dependency property: the trust score of the data affects the trust score of the network nodes that created and manipulated the data, and vice-versa.

IV. PROPOSED SYSTEM

We are designing a provenance encoding and decoding mechanism that satisfies security and performance needs. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node.

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

ADVANTAGES OF PROPOSED SYSTEM:

1. Our design is efficient techniques for provenance decoding and verification at the base station.
2. We extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
3. We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.
4. We only require a single channel for both transmission channels for data and provenance.

V. SYSTEM ARCHITECTURE

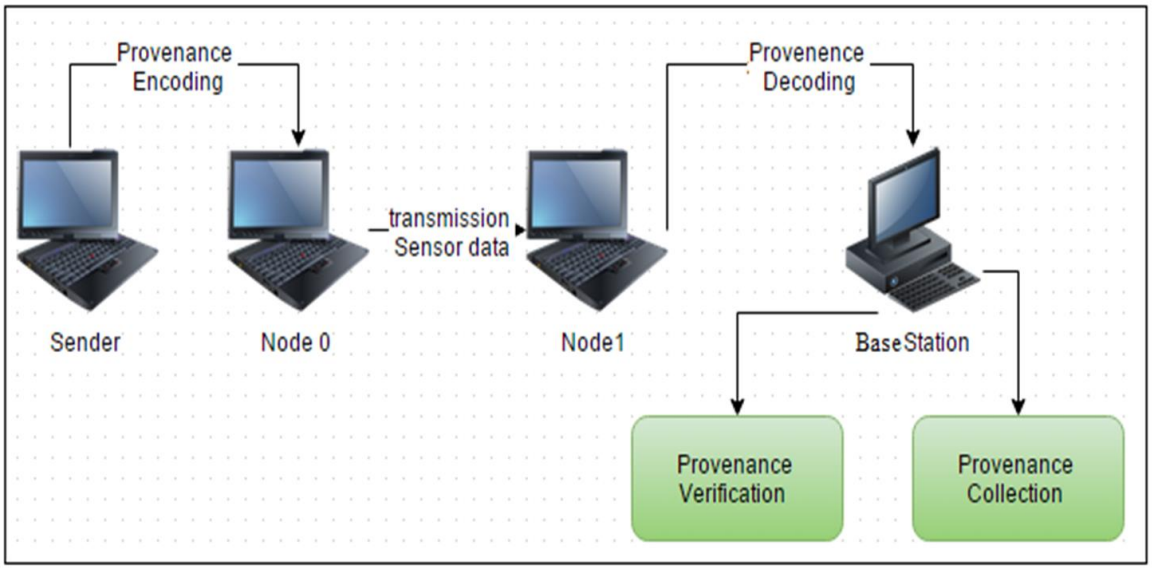


Figure 5.1. Block diagram of system architecture

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} .

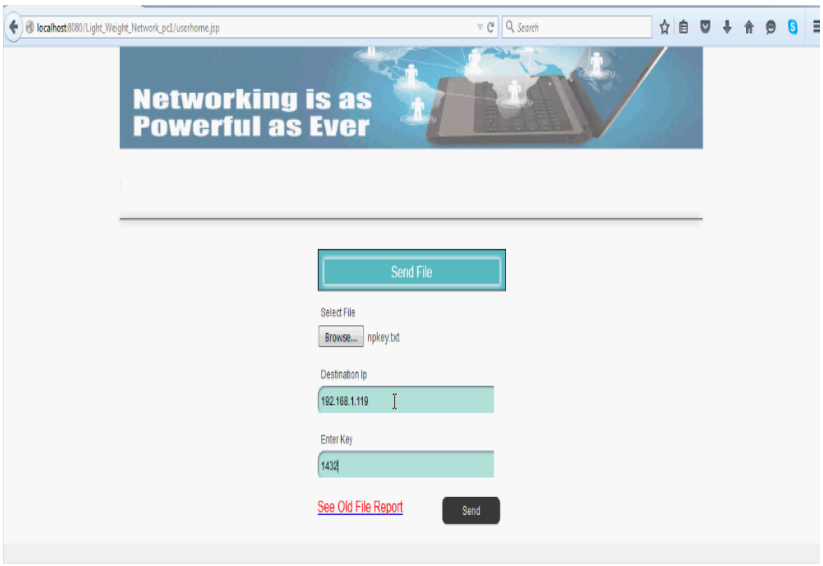
5. E is edge set consists of directed edges that connect sensor nodes.

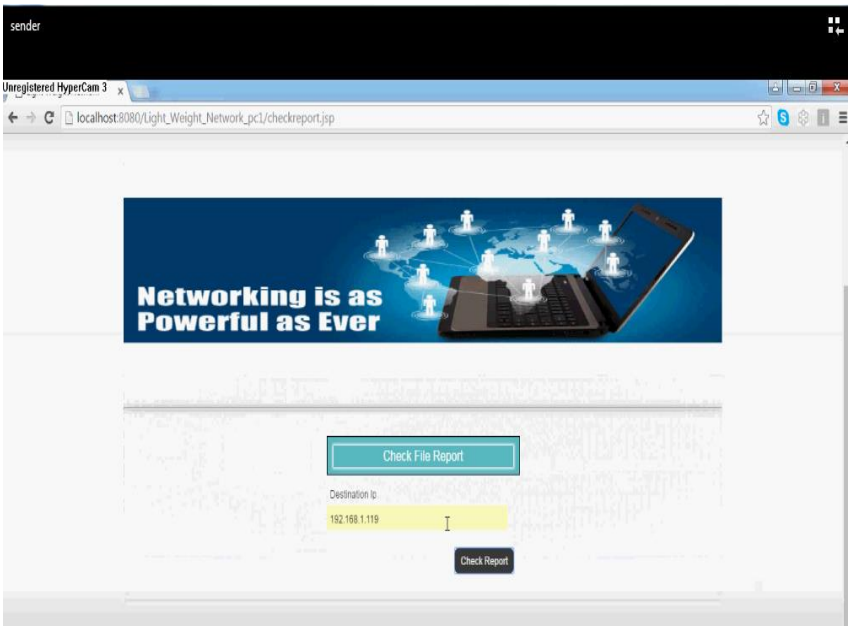
6. d is the set of data packets,

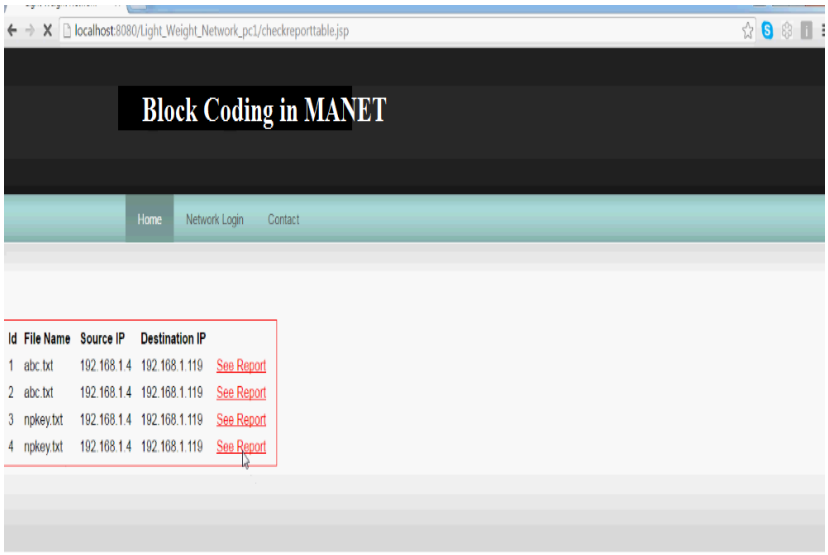
Let G is acyclic graph G(V,E) where each vertex v ∈ V is attributed to a specific node HOST(v) = n and represents the provenance record (i.e. nodeID) for that node.

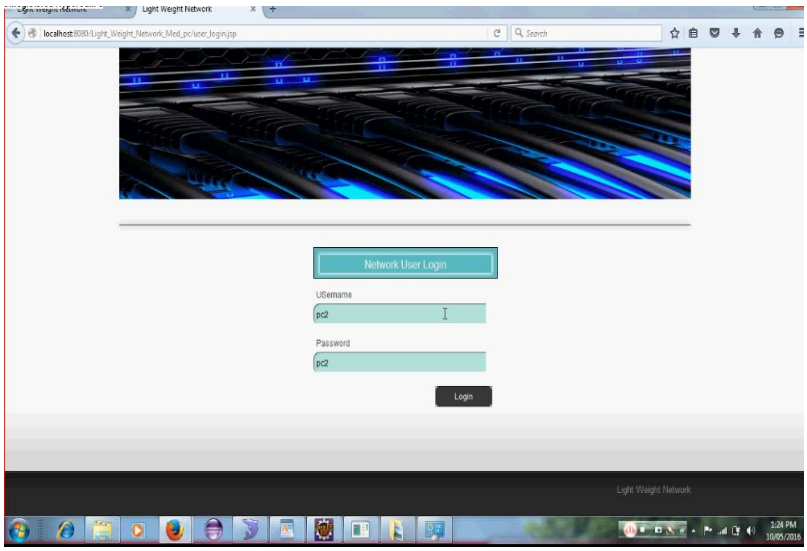
Each vertex in the provenance graph is uniquely identified by a vertex ID (VID) which is generated by the host node using cryptographic hash functions.

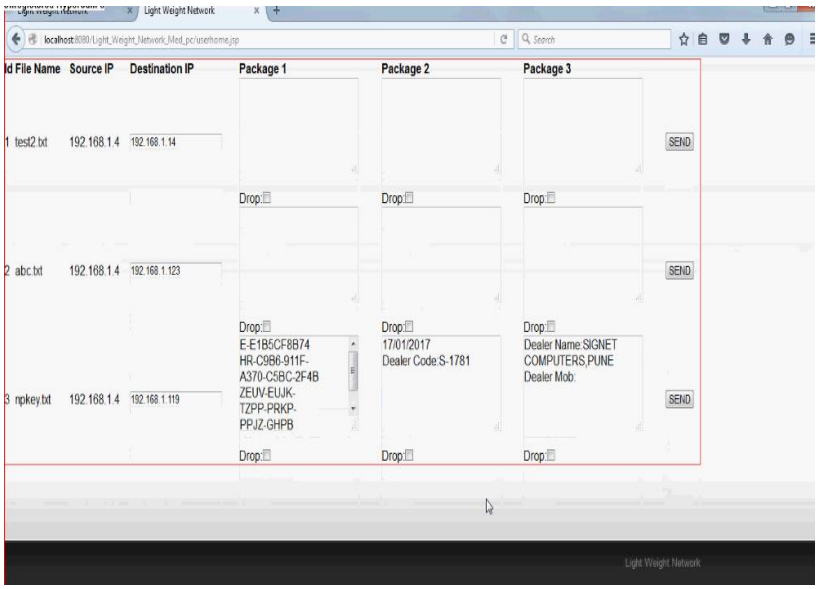
VII. RESULT SET

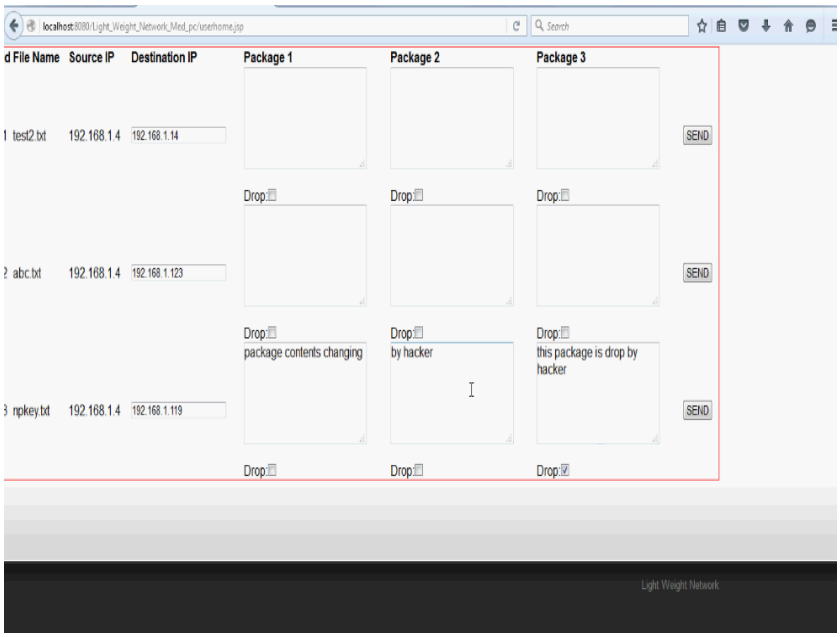


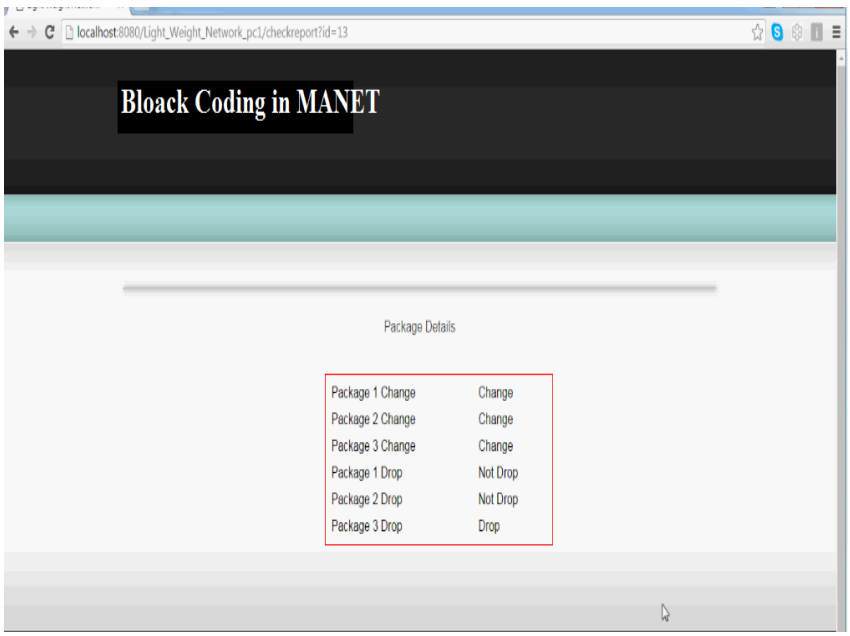


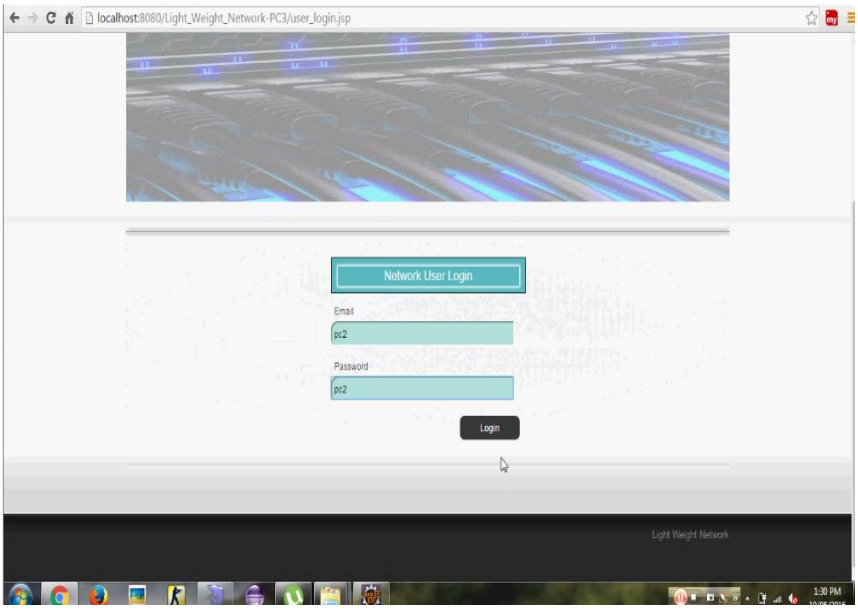


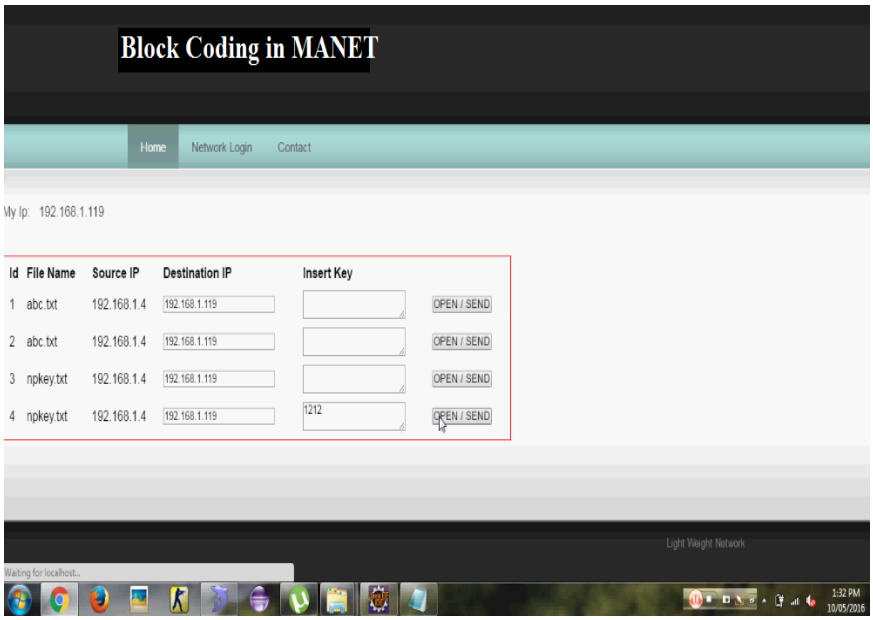


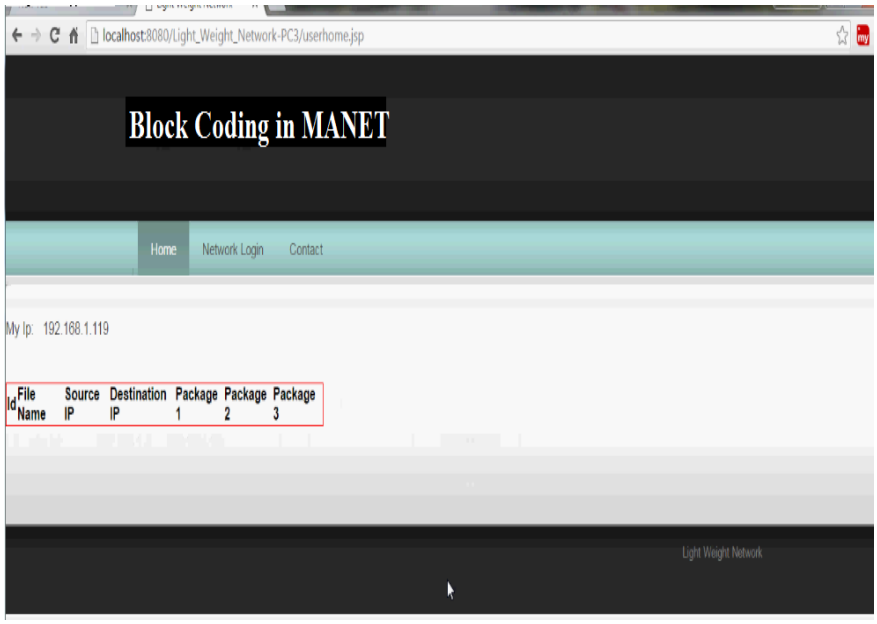


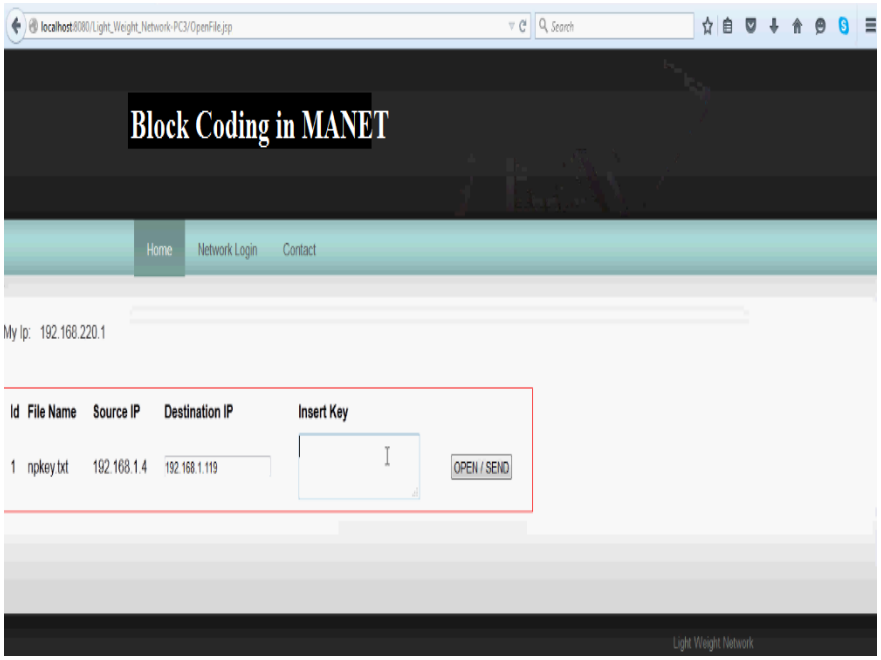












VIII. CONCLUSION

We addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

IX. REFERENCES

1. Salmin Sultana, Gabriel Ghinita, Member, IEEE , Elisa Bertino, Fellow, IEEE , and Mohamed Shehab, Member, IEEE Computer Society, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015.

2. 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.

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

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

6. 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.

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