A Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks

[1]Prof. Pate Sumeet, [2]Mr. Patel Khush M, [3]Mr. Gohil Darshan, [4]Mr. Sondkar Bhushan R

[1]Asst. Professor, [2,3,4]UG Student, [1,2,3,4]Computer Engg. Dept. Shivajirao S.Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

[1]sumeetpate09@gmail.com, [2]kp1241996@gmail.com, [3]darshangohil234@gmail.com, [4]bhushansondkar@gmail.com

Abstract— Large-scale sensors are deployed in application domains, and the data which is collected are used to make specific decisions for critical infrastructures. Data is collected from different sources through intermediate processing nodes that aggregate information. A malicious adversary may add new nodes in the network which compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Provenance management for device networks introduces many difficult necessities, like low energy and information measure consumption, economical storage and secure transmission. This paper proposes a unique light-weight theme to firmly transmit origin for device knowledge. The papered technique depends on in packet Bloom filters to cypher origin. This paper introduces economical mechanisms for origin verification and reconstruction at the bottom station. Additionally, it extends the secure origin theme with practicality to sight packet drop attacks staged by malicious knowledge forwarding nodes. This paper measure the papered technique each analytically and through empirical observation, and therefore the results prove the effectiveness and potency of the light-weight secure origin theme in sleuthing packet forgery and loss attacks.

Keywords— Provenance, Security, Sensor Networks.

I. INTRODUCTION

Sensor networks are used in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. data is being produced which is to be transferred from the base station that is the sender to the receiver end. Data are made at a large scale of different node sources and made to transfer from base station to the receiver end. In decision making process only trustworthy information is considered. The provenance is made to assess data specification which leads to the summarization of the actions to be perform on data. Recent research shows that if any illegal data is being processed using provenance, it may lead to data failure. Provenance is being studied throughout for collection, querying but in sensor network it is not used specifically. The use of provenance to detect packet loss and forgery in a particular system which are being staged by malicious node.

The paper contains the data which are to be transfer from the base station to the receiver's end which are to be cumulated into different packet through which data is transferred. The data which is being transferred is under thread of being attack. This may lead to data loss or different modification in the data which is being transferred. To create a particular secure scheme which may result to the secure transmission of the data. In this scheme the data from the base station to the receiver end is transferred securely without any packet loss or modification. It also try to make a particular scheme which identifies if particular packet is being attack or modified which is stage to malicious node.

As opposed to existing research that employs separate transmission channels for data and provenance, it only requires a single channel for both. Furthermore, traditional Provenance security solutions use intensively cryptography and digital signatures [5], and they employ append-based data structures to store provenance, leading to prohibitive costs. In contrast, use only fast Message Authentication Code (MAC) schemes and Bloom filters (BF), 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.

II. LITERATURE SURVEY

Cryptography

Cryptography is basic procedure of creating plain text into cypher text which tries to make a secure transmission the data converted into cypher text is never been in same manner. It has particular aspect such as data confidentiality, data integrity, authentication, non-repudiation. Cryptography is used for ATM card, creating passwords and electronic use.

A. Key generation.

There are two types of key, which are public and private. The public key is used for encryption of data whereas the private key is used for decryption.

Cryptography is a techniques for secure communication in the presence of third parties. Cryptography is used for changing the plaintext into cipher text. Cryptography is used for data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

1. Encryption

Alice transmits her public key (n,e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. Alice first turns M into an integer m, such that 0≤m<nby using an agreed-upon reversible protocol known a a padding scheme. He then computes the cipher text corresponding to c=me(mod n) This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

B. Decryption

Alice can recover m from c by using her private key exponent d via computing m=cd (mod n). Given , she can recover the original message M by reversing the padding scheme[i]..

III. Proposed System

The data which needs to be transferred from the sender to the receiver needs to be secure. The attacks which may be occurred at the provenance of the node or any of the packets which are being transferred which my lead to data loss. The goal of this paper is to create a secure transmission which may stop data loss are any provenance forgery. It proposed provenance encoding strategy whereby each node on the path of data packet securely embeds provenance information with in a bloom filter that is transmitted along with the data.

The data upon receiving from the sender to the receiver extracts the provenance information. It verifies the data which is being received. It checks the provenance information, whether any attack has been occurred or any packet is been dropped. It also devise an extension of the provenance encoding scheme that allows the base station to detect if a packet drop attack was staged by a malicious node.

IV. System Architecture

This paper introduces about A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks. The service provider starts to search for all possible nodes through which data could be transferred securely and effectively to the receiver end. The data is send through nodes which are available through routers. It will first try to check the nodes which are being dropped or modified, due to which data doesn’t reach to the receiver appropriately. It will apply filtering techniques on the nodes which are being dropped or modified, through which approximate data loss can be configured. This configured data checked through filter states the location nodes where the attack is occurred. Then the location node where the attack is occurred is updated and the node is been changed for the transfer of data. This data which is being transferred through updated node reaches to the receiver end successfully without any data dropped or modified.

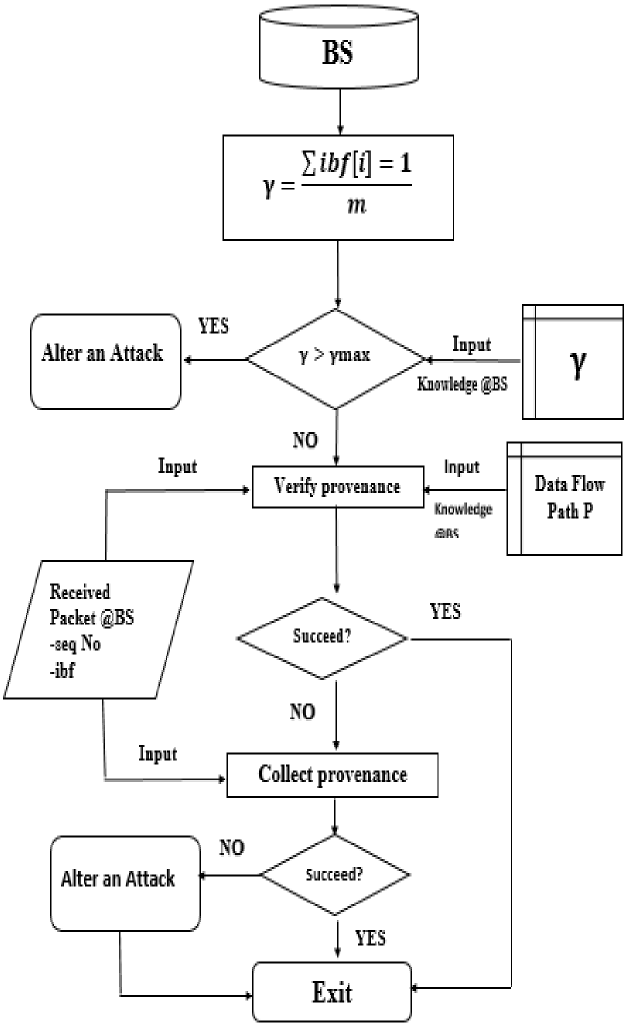


Fig. 1. Provenance processing workflow at the BS upon receiving a packet

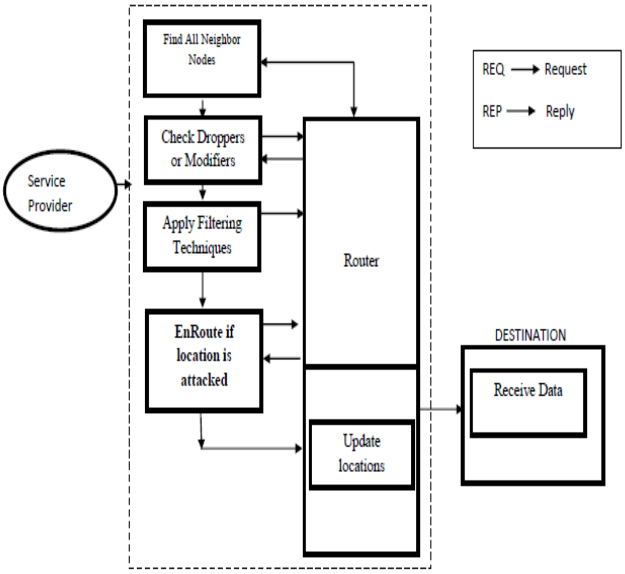


Fig. 2. System Architecture

Table 1. Comparative Study

SR NO	Paper Title	Author's Name	Problem	Solution	Future Work
1.	Secure and Efficient Key Management in Mobile Ad Hoc Networks	Bing Wu, Jie Wu, Eduardo B. Fernandez	Public key infrastructure (PKI) is not secure for encryption	Secure and efficient key management (SEKM) is provided in which ticket scheme is introduce for efficient certificate service.	The performance of SEKM by simulation, and it extend SEKM to multiple server groups in large n/w
2.	Spatial Signatures for Lightweight Security in Wireless Sensor Networks	Lifeng Sang and Anish Arora	The potentially large number and dynamic nature of nodes pose a hard key management	A lightweight and robust primitive that validates the spatial signature of messages at run-time.	Consideration of crypto-free alternative for other security services including privacy.
3.	Access points vulnerabilities to DoS attacks in 802.11 networks	F. Ferreri and M. Bernaschi	Denial of service attacks.	serious vulnerabilities in different access point and a single malicious station can easily hinder any legitimate communication within Service	802.11n adoption will greatly extend the range of this network.
4.	A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks	Salmin Sultana,Gabriel Ghinita.	Attacks in the starting of transmission may lead to loss packets.	Sensor node is provided at the starting of the transmission which acknowledge about the packet drop attacks and forgery attack.	Implementing secure scheme to improve the accuracy of packet loss in malicious sensor nodes.

V. ALGORITHM

Algorithm 1 AES ENCRYPTION

```
encrypt(data,string)
{
keyWord = keyWord.substring(0, 16);
          byte[] keyValue = keyWord.getBytes();
          System.out.println("Size : " + keyValue.length);
          Key key = new SecretKeySpec(keyValue, ALGO);
                    Cipher c = Cipher.getInstance(ALGO);
                    c.init(Cipher.ENCRYPT_MODE, key);
String              encryptedValue           =          new
String(Base64.encode(Data.getBytes()));
                    return encryptedValue;
}
```

Algorithm 2 AES DECRYPTION

```
decrypt(data,string)
{
keyWord = keyWord.substring(0, 16);
          byte[] keyValue = keyWord.getBytes();
          Key key = new SecretKeySpec(keyValue, ALGO);
                    Cipher c = Cipher.getInstance(ALGO);
                    c.init(Cipher.DECRYPT_MODE, key);
String              decryptedValue           =          new
String(Base64.decode(encryptedData.getBytes()));
                    return decryptedValue;
}
```

VI. MATHEMATICAL MODEL

Space Complexity

Since the approach is based on the BF, the provenance length depends on parameter selections for the BF. The false positive probability for a BF is defined as [21]

$$Pfp\frac{na-n}{nt-n}$$

where n_t is the total number of distinct elements in the element space, n is the number of elements actually encoded in the BF and n_a is the number of elements retrieved by querying the BF.

Energy Consumption

For a D-hop path, SSP has to transmit $42*D$ bytes $(= 336*D$ bits), MP transmits $6*D$ bytes $(= 48*D$ bits $)$ whereas the scheme requires transmitting m bits. SSP, MP and other scheme consume a radio energy proportional to $(336*D)$, $(48*D)$ and $\frac{ln\frac{1}{\delta}}{(ln2)^2}*D$, respectively. Although all of the terms are proportional to D, the constant coefficient in the first two terms is much larger than the last one.

Detection of Packet Drop Attacks

Theorem 1: Given the threshold $\alpha = \rho + \varepsilon$ and the allowed false positive σ, the scheme requires

$$\frac{ln(\frac{2}{\sigma})}{2\varepsilon^2(1-\rho-\varepsilon)^D}$$

Packets to be transmitted by the source to achieve the converging condition.

This paper define each instance of a data packet arriving at node n_i as a random variable of l_i. It assume that a node correctly embeds its provenance record whenever it forwards a data packet. Using Maximum Likelihood Estimation and Hoeffding's inequality, obtain

$$Pr(|r_i^* - r_i| > \varepsilon_{r_i}) \le 2\exp\ -2N_i\varepsilon_{r_i}^2$$

$$\Rightarrow N_i = \frac{ln(\frac{2}{\sigma})}{2\varepsilon_{r_i}^2} \ge \frac{ln(\frac{2}{\sigma})}{2\varepsilon^2}$$

Now to compute the number of packets needed to give an estimate with ($\_{ri}$, σ)-accuracy for every link in a D-hop path. When each packet transmitted by the source reaches node $n_{(D-1)}$, it

provides a trial for every link l_i belonging to the path. Therefore, transmitting N_i packets to $n_{(D-1)}$ also suffices to give other links enough trial Which requires a total of

$$N_{(D-1)}\frac{1}{(1-\alpha)^D} = \frac{ln(\frac{2}{\sigma})}{2\epsilon^2(1-\rho-\epsilon)^D}$$

Packet transmitted from the source.

VII. EXPECTED RESULT

The paper "a light weight secure scheme for detecting provenance forgery and packet drop attack" contains the result such as the pckets which are being transferred from sender to the receiver is protected. The packets which are send can be attack by intruders, which are being protected. In this pr the packet are being secure from attackers. The packets which are being modify by the attacker are saved without getting them to be modified.

VIII. ANALYSIS OF PROJECT

The paper "a light weight secure scheme for detecting provenance forgery and packet drop attack" contains the result of the paper. The analysis of the paper is also shwon accordingly. The analysis is shown through graph which contains the total result of the paper. The graph are of two types, one is of packet attacker and other is of packet modifier.

The packet attacker graph shows how many times the transfer of data packet is been attack. The number of packets being attack or lost during attack are shown in the graph. Similarly the packets which are tried to modify through other circumstances are also shwon in the graph. If the attack is occurred in which the packets are modified the graph shows all the analysis of the paper.

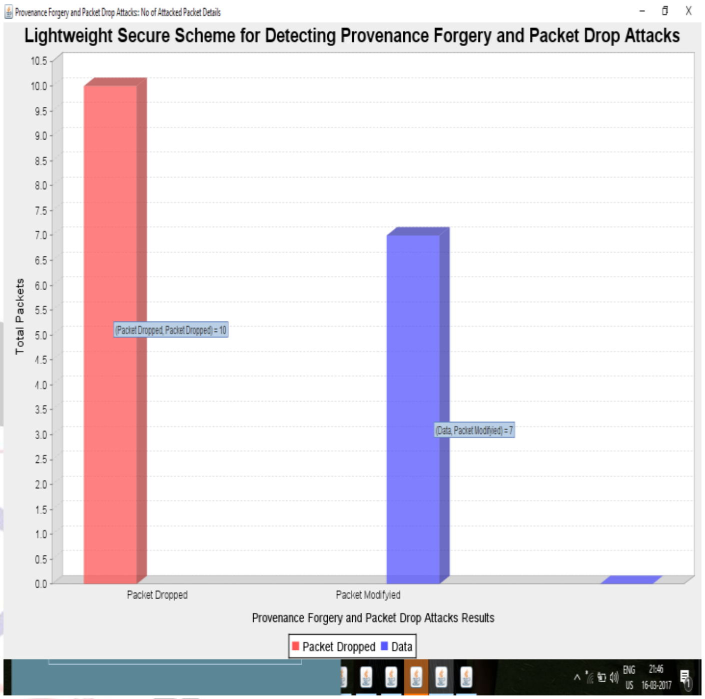
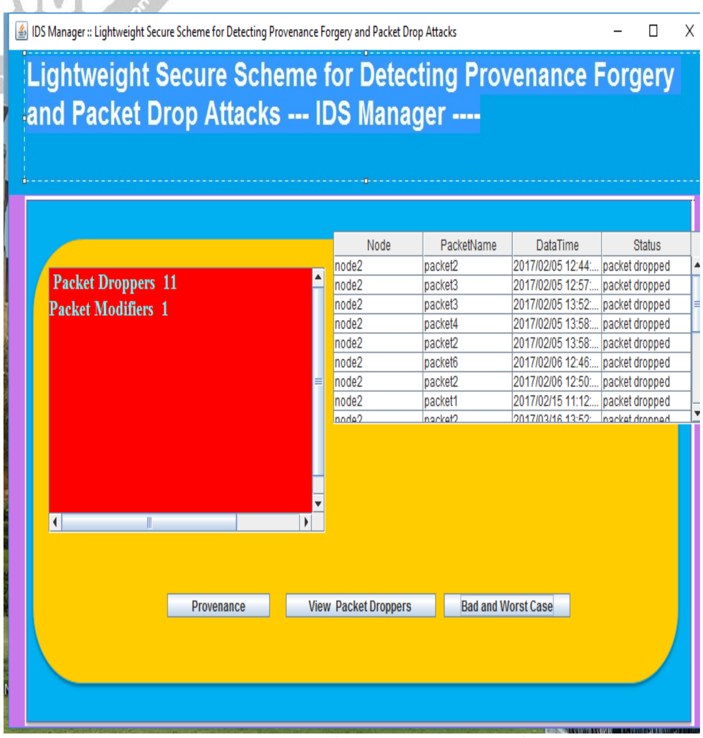


Fig. 3. Analysis of project


IDS Manager :: Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks

Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks --- IDS Manager ----

Packet Droppers 11
Packet Modifiers 1

Node	PacketName	DataTime	Status
node2	packet2	2017/02/05 12:44:...	packet dropped
node2	packet3	2017/02/05 12:57:...	packet dropped
node2	packet3	2017/02/05 13:52:...	packet dropped
node2	packet4	2017/02/05 13:58:...	packet dropped
node2	packet2	2017/02/05 13:58:...	packet dropped
node2	packet6	2017/02/06 12:46:...	packet dropped
node2	packet2	2017/02/06 12:50:...	packet dropped
node2	packet1	2017/02/15 11:12:...	packet dropped
node2	packet2	2017/03/16 13:52:...	packet dropped

Fig. 4. Count of attackers and modifier

IX. DESIGN DETAILS

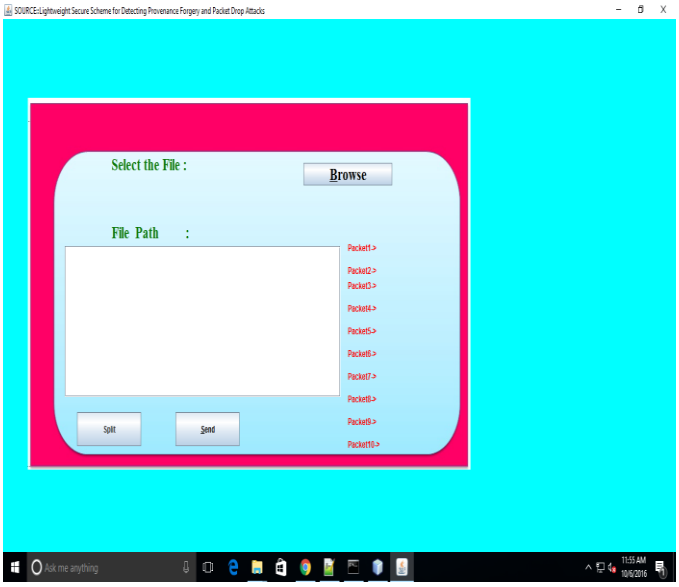


Fig. 5. Home page of detection and prevention

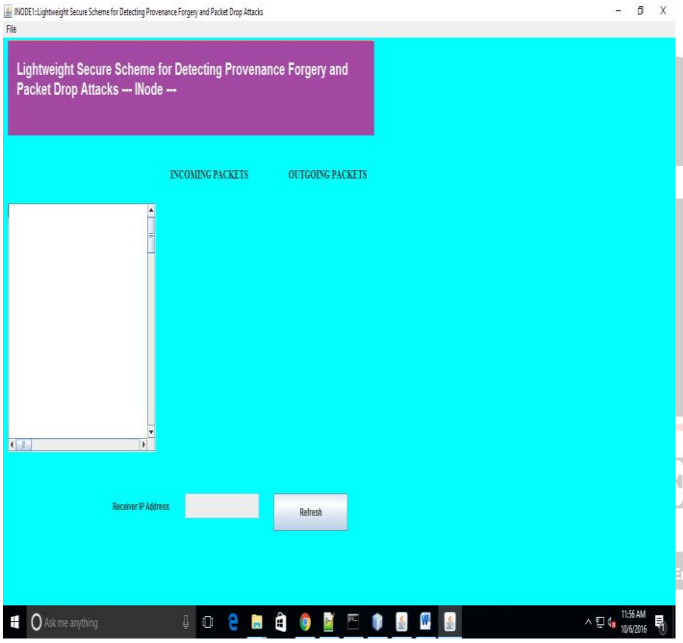

INODE1::Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks
File
Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks --- INode ---
INCOMING PACKETS
OUTGOING PACKETS
Receiver IP Address
Refresh
Ask me anything
11:56 AM
10/6/2016

Fig. 6. first node of detection and prevention

X. CONCLUSION

We have tried to implement the paper "Salmin Sultana, Gabriel Ghinita, Elisa Bertino, Mohamed Shehab", "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks", IEEE 2013, and according to the implementation the conclusion is that it addresses the matter of firmly transmittal provenance for sensing element networks, and planned a light-weight provenance encryption and coding theme supported Bloom filters. The theme ensures confidentiality, integrity and freshness of provenance. It have a tendency to extend the theme to include data-provenance binding, and to incorporate packet sequence data that supports detection of packet loss attacks. Experimental and analytical analysis results show that the planned theme is effective, light-weight and ascendable. In future work, to have a tendency to implement a true system prototype of our secure provenance theme, and to enhance the accuracy of packet loss detection, particularly within the case of multiple consecutive malicious sensing element nodes.

REFERENCES

[1] Salmin Sultana, Gabriel Ghinita, Mohamed Shehab and Elisa Bertino, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks," IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, Jan. 2013

[2] 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.

[3] 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

[4] 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.

[5] 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.

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

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.