International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Vol.05,Issue.01,
January-2017,
Pages:0018-0022

A Translucent and Safe Strategy for Identifying the Root Cause of Replication and Counterfeit Attacks in WSN

AYESHA FIRDOUS[1], SARA ALI[2]
[1]PG Scholar, Dept of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, TS, India.
[2]Associate Professor, Dept of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, TS, 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. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

Keywords: Provenance, Security, Sensor Networks.

I. INTRODUCTION

Sensor systems are turning out to be progressively well known in various application areas, for example, digital physical base frameworks, natural observing, power matrices, and so forth. Information are delivered at a substantial number of sensor hub sources and prepared in-system at transitional bounces on their way to a base station that performs basic leadership. The differing qualities of information sources make the need to guarantee the reliability of information, such that exclusive dependable data is considered in the choice procedure. Information provenance is a powerful technique to survey information reliability, since it abridges the historical backdrop of proprietorship and the activities performed on the information. Late research highlighted the key commitment of provenance in frameworks where the utilization of deceitful information may prompt calamitous disappointments e.g. SCADA frameworks for basic base. Despite the fact that provenance displaying, gathering, and questioning have been researched widely for work processes and curate databases, provenance in sensor systems has not been legitimately tended to. In this paper, we explore the issue of secure and productive provenance transmission and preparing for sensor systems. In a multi-jump sensor system, information provenance permits the base station to follow the source and sending way of an individual information bundle since its era. Provenance must be recorded for every information bundle; however imperative difficulties emerge because of the tight stockpiling, vitality and transmission capacity requirements of the sensor hubs. Hence, it is important to devise a light-weight provenance arrangement which does not present noteworthy overhead.

Moreover, sensors regularly work in a UN trusted situation, where they might be liable to assaults. Consequently, it is important to address security necessities, for example, classification, honesty and freshness of provenance. We will likely plan a provenance encoding and disentangling instrument that fulfills such security and execution needs. We propose a provenance encoding technique whereby every hub on the way of an information parcel safely implants provenance data inside a Bloom channel, which is transmitted alongside the information. After getting the information, the base station extricates and checks the provenance. Sensor systems are utilized as a part of various application domains, such as digital physical base frameworks, environmental monitoring, power lattices, and so forth. Information are delivered at a large number of sensor hub sources and prepared in-system at intermediate bounces on their way to a Base Station (BS) that performs decision-making. The assorted qualities of information sources create the need to guarantee the dependability of data, such that lone reliable data is considered in the decision process. Information provenance is a compelling method to survey information trustworthiness, since it compresses the history of possession and the activities performed on the data. Late research highlighted the key commitment of provenance in frameworks where the utilization of conniving data may lead to disastrous disappointments (e.g., SCADA systems).

Although provenance demonstrating, gathering, and querying have been concentrated widely for work processes and curate databases, provenance in sensor systems has not been appropriately tended to. We research the issue of secure and effective provenance transmission and processing for sensor systems, and we utilize provenance to identify packet loss assaults arranged by malevolent sensor hubs. In a multi-jump sensor system, information provenance allows the BS to follow the source and sending way of an individual information parcel. Provenance must be recorded for each parcel, yet critical difficulties emerge due to the tight storage, vitality and transmission capacity imperatives of sensor hubs. Along these lines, it is important to devise a light-weight provenance solution with low overhead. Moreover, sensor soften operate in an entrusted domain, where they may be subject to assaults. Consequently, it is important to address security requirements, for example, classification, honesty and freshness of provenance. We will probably outline a provenance encoding and disentangling system that fulfills such security and performance needs. We propose a provenance encoding strategy whereby every hub on the way of an information packet securely installs provenance data inside a Bloom filter that is transmitted alongside the information. Upon receiving the parcel, the BS separates and confirms the provenance information. We likewise devise an expansion of the provenance encoding plan that permits the BS to identify if a packet drop assault was arranged by a pernicious node. As restricted to existing examination that utilizes separate transmission channels for information and provenance, we only require a solitary channel for both. Moreover, traditional provenance security arrangements utilize seriously cryptography and advanced marks, and they utilize affix based data structures to store provenance, prompting prohibitive costs. Conversely, we utilize just quick Message Authentication Code (MAC) plans and Bloom channels (BF), which are fixed-size information structures that minimally speak to provenance. Bloom channels make proficient use of bandwidth, and they yield low mistake rates by and by.

II. EXISTING AND PROPOSED SYSTEMS

A. Existing System

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

Disadvantages of Existing System:

- Any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys.
- User revocation is not supported in their scheme.

B. Proposed System

In proposed system using key exchanging, cryptography, and signature technique are used. So easily detect the suspicious data. In verify module detect the suspicious data and provenance data. Receiving packet data suspicious data means placed in suspicious box as shown in Fig.1. Suppose data will be provenance data means placed in provenance box.

Advantages of Proposed System:

- Any user in the group can store and share data files with others by the cloud.
- The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
- User revocation can be achieved without updating the private keys of the remaining users.

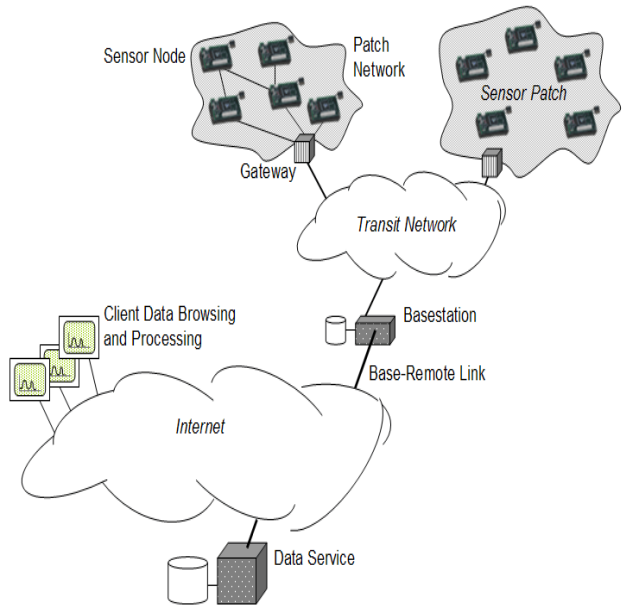

Fig.1. System Architecture.

III. DETECTING PACKET DROP ATTACKS MECHANISM

We extend the secure provenance encoding scheme to detect packet drop attacks and to identify malicious node(s). We assume the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, we consider only linear data flow paths. Also, we do not address the issue of recovery once a malicious node is detected. Existing techniques that are orthogonal to our detection scheme can be used, which may initiate multipath routing or build a dissemination tree around the compromised nodes. We augment provenance encoding to use a packet acknowledgement that requires the sensors to transmit more meta-data. For a data packet, the provenance record generated by a node will now consist of the node ID and an acknowledgement in the form of a sequence number of the lastly seen (processed/forwarded) packet belonging to that data flow. If there is an intermediate packet drop, some nodes on the path do not receive the packet. Hence, during the next round of packet transmission, there will be mismatch between the acknowledgements generated from different nodes on the path. We utilize this fact to detectthe packet drop attack and to localize the malicious node. We consider a data flow path P

where nlis the only data source. We denote the link between nodes ni and n(i+1)as li. We describe next packet representation, provenance encoding and decoding for detecting packet loss.

A. Data Packet Representation

To enable packet loss detection, a packet header must securely propagate the packet sequence number generated by the data source in the previous round. In addition, as in the basic scheme, the packet must be marked with a unique sequence number to facilitate per-packet provenance generation and verification.

B. Provenance Encoding

It depicts the extended provenance encoding process. The provenance record of a node includes (i) the node ID, and (ii) an acknowledgement of the lastly observed packet in the flow. The acknowledgement can be generated in various ways to serve this purpose.

C. Provenance Decoding at the BS

Not only the intermediate nodes, but also the BS stores and updates the latest packet sequence number for each dataflow. Upon receiving a packet, the BS retrieves the preceding packet sequence (pSeq) transmitted by the source node from the packet header, fetches the last packet sequence for the flow from its local storage (pSeqb), and utilizes these two sequences in the process of provenance verification and collection.

IV. SIMULATION RESULTS

We implemented and tested the proposed techniques using the Tiny OS simulator (TOSSIM). We have used chemical energy model and Power TOSSIM z plug-in tootsie to measure the energy consumption. We consider a network of 100 nodes and vary the network diameter from 2 to 14. All results are averaged over 100 runs. First, we look at how effective the secure provenance encoding scheme is in detecting provenance forgery and path changes. Next, we investigate the accuracy of the proposed method for detecting packet loss.

A. Provenance Decoding Error

Provenance decoding retrieves the provenance from the in packet BF and consists of verification and collection phases. To quantify the accuracy and efficiency of our provenance scheme, we measure the decoding error in both the above phases, i.e., verification and collection error. Algorithm 1 shows that the verification fails when the provenance graph in the packet does not match the local knowledge at the BS. This may happen when there is a data flow path change or upon a BF modification attack. Provenance verification failure rate (VFR) measures the Ratio of packets for which verification fails. Fig. 2(a) shows the VFR for paths of 2 to 12 hops with various BF sizes. For each path length, the VFR is averaged over 1000 distinct paths. The results show that the provenance verification process fails only for a very small fraction of packets. Thus, for most packets the lightweight verification process is sufficient to retrieve the provenance. On the other hand, VFR is not significantly influenced by BF size, proving that even small BF sizes provide good protection. Fig 2(b) shows the variation of VFR over time, as the number of packet transmissions increases. As the network gets stable with time, the data paths do not change often and hence the VFR approaches 0.

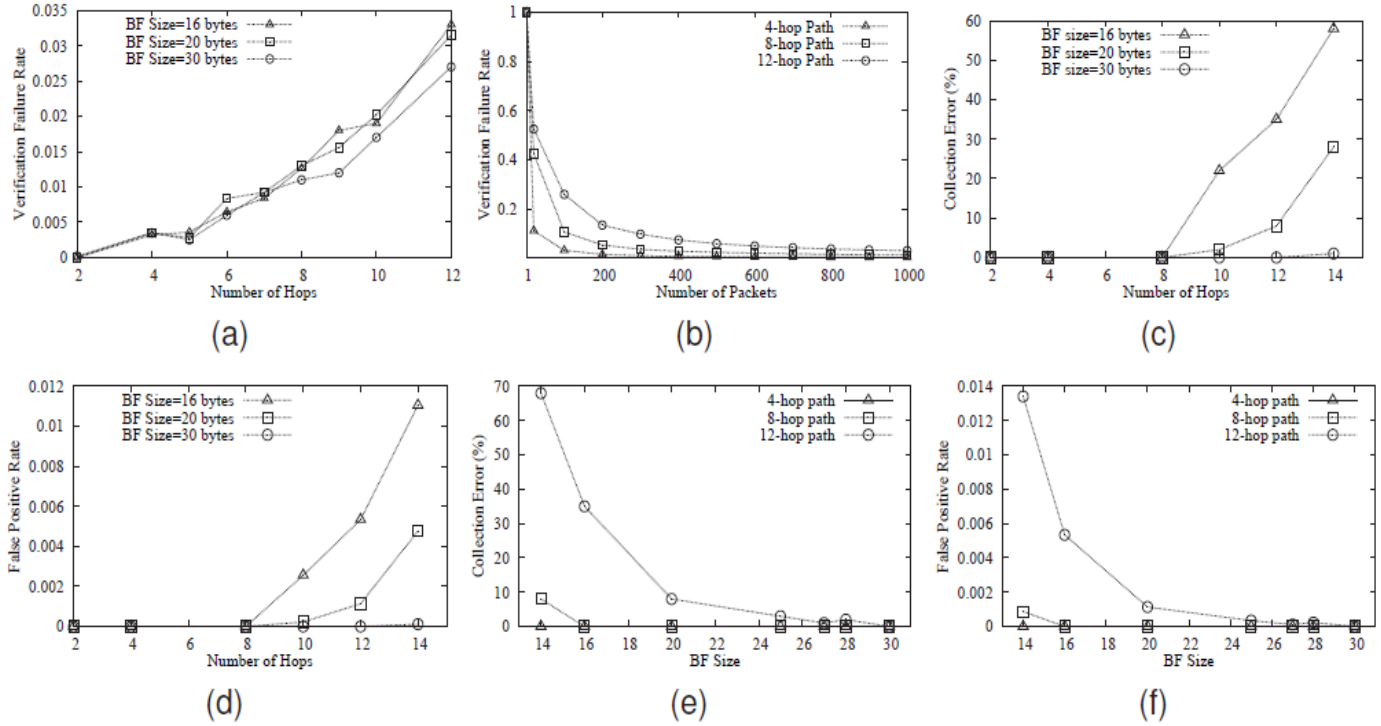

Fig.2. (a) Provenance VFR vs path length. (b) VFR variation with time as network stabilizes. (c)(d)(e)(f)Collection Error and False Positive Rate for various path lengths and BF sizes.

Fig. 2(c) and 2(d) plot the percentage of provenance collection error for different number of hops and the corresponding BF false positive rates, respectively. Recall that, the collection phase is executed when provenance verification fails. Fig. 2(e) and 2(f) show the collection error corresponding to various BF sizes and the related false positives, respectively. The resulting false positive rates vary from 0 ~0.013 and it is observed that the collection error becomes negligible when the false positive rate drops at or below 10^{-4}. It is also seen that a BF size of 16 bytes is enough to ensure no decoding error for up to8-hop paths. The empirical BF size required is much less than the theoretical one (~20 bytes for an 8-hop path).

B. Detection of Packet Drop Attacks

In these experiments, we consider one malicious node in every data path considered, the natural link loss rate is set-to ρ = 0.01, the malicious link loss rate to α = 0.06, and the maximum allowed threshold for false positives in attack detection to σ = 0.03. The BF sizes are varied from16 to 35 bytes (note that this is slightly larger than for

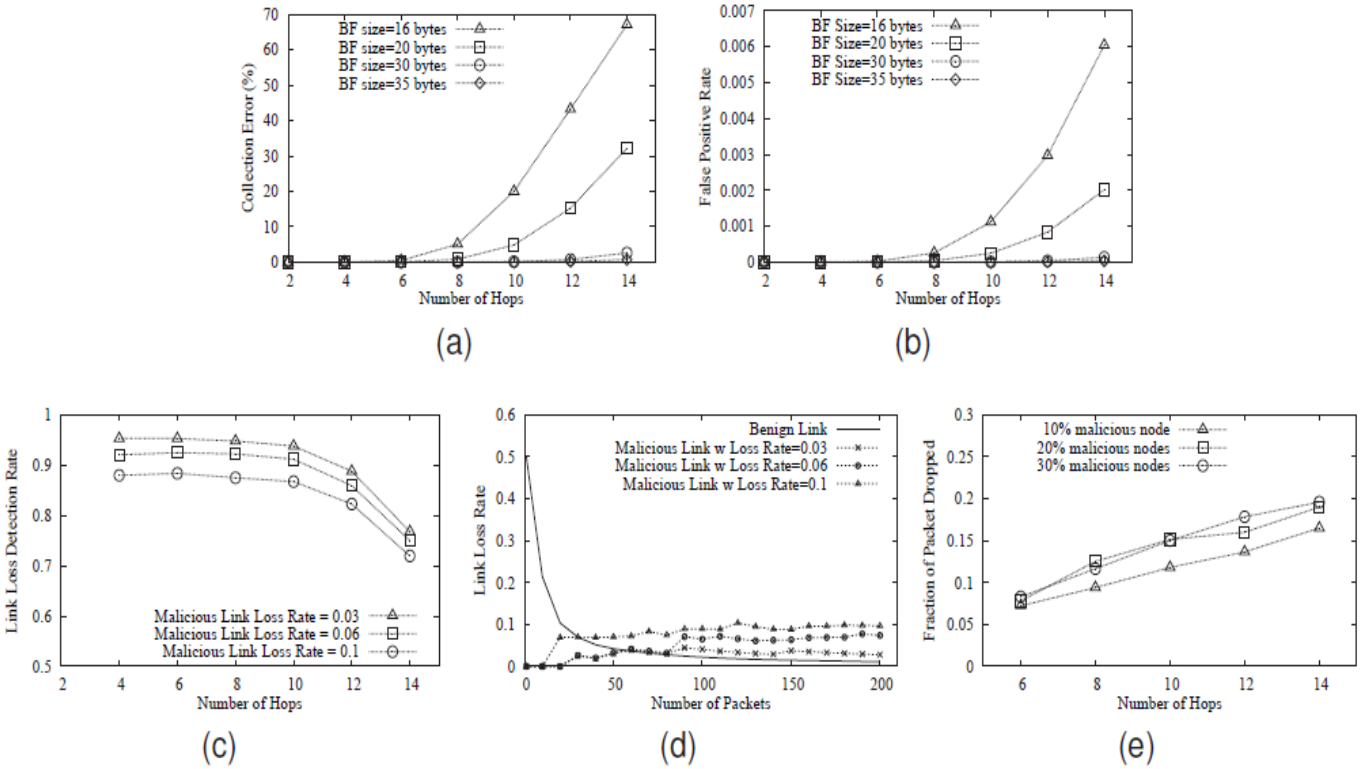

Fig.3. (a) Percentage of Collection Error (b) False Positive Rates of extended provenance scheme. (c) Success rate of detecting packet drop for various malicious link loss rates. (d) Accuracy of malicious link identification overtime. (e) End-to-end packet drop rate for various percentages of malicious nodes deployed in the network.

The basic scheme, because the packet sequence information must now be included as well in the BFs). The percentages of provenance collection error and corresponding false positive rates for the extended provenance scheme are shown in Fig. 3(a) and 3(b), respectively. Fig. 3(a) shows that the provenance collection error for the extended scheme depends on BF sizes and follows the same pattern as in the basic scheme. As expected, the errors for the same BF sizes are higher compared to the basic scheme; due to the extended (doubled) element space for the received iBFwhich increases the hash collisions and consequently the error rates. With a suitably chosen BF size (e.g. 30 bytes); collection errors can be kept low for any path lengths. Thus, the collection error does not affect much the accuracy of the malicious node identification process. The false positives in the error cases, as shown in Fig. 3(b), do not have significant changes compared to those of the basic scheme. Fig. 3(c) illustrates the success of our provenance scheme in detecting packet losses. Rate. Fig. 3(d) shows the accuracy of the malicious link identification process over time and how it leads to the detection of packet drop attacks. Fig. 3(e) presents the degradation of data throughput by the time the attack is detected in robust settings, where 10%, 20%, and 30% of the total nodes are malicious. As expected, the data throughput at the BS degrades with the increasing number of malicious nodes in the data flow path.

C. Space Complexity and Energy Consumption

Fig. 4(a) compares SSP, MP and our provenance mechanism in terms of bytes required to transmit provenance. The provenance length in SSP and MP increases linearly with the path length. For our scheme, we empirically determine the BF size which ensures no decoding error. We also measure the energy consumption for both the basic provenance scheme and the extended scheme for packet drop detection, while varying hop counts. For packet Drop attack, we set the

malicious link loss rate as 0.03. Note that, modern sensors use ZigBee specification for high level communication protocols which allows up to 104 bytes as data payload. Hence, SSP and MP can be used to embed provenance (in data packet) for maximum 2 and 14 nodes, respectively. Fig.4 (b) shows aggregate energy consumption over 1000 packet transmissions. The results confirm the energy efficiency of our solutions.

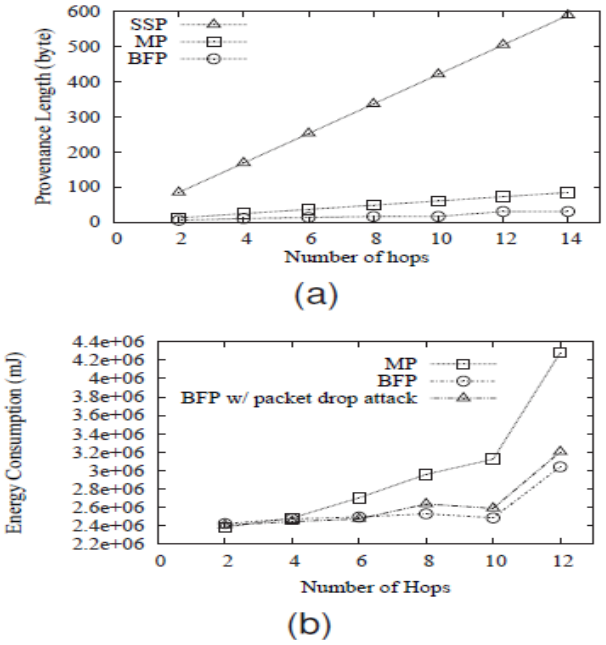

Fig.4. (a) Provenance length (b) Energy consumption.

V. CONCLUSION

We tended to the issue of safely transmitting provenance for sensor organizes, and proposed a light-weight provenance encoding and unraveling plan in view of Bloom channels. The plan guarantees privacy, uprightness and freshness of provenance. We extended the plan to join information provenance official, and to incorporate parcel succession data that backings recognition of bundle misfortune assaults. Test and investigative assessment results demonstrate that the proposed plan is powerful, light-weight and adaptable. In future work, we plan to actualize a genuine framework model of our safe provenance plot, and to enhance the precision of parcel misfortune recognition, particularly in the instance of numerous successive malevolent sensor hubs.

VI. REFERENCES

[1] Salmin Sultana,Gabriel Ghinita, Member, IEEE, Elisa Bertino, Fellow, IEEE,and Mohamed Shehab, Member, IEEE,"A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing Vol. 6, No. 1, January 2015.

[2] H. Lim, Y. Moon, and E. Bertino, "Provenance-based trustworthinessassessment in sensor networks," in Proc. of Data Management forSensor Networks, 2010, pp. 2–7.

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

[4] 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.

[5] Y. Simmhan, B. Plale, and D. Gannon, "A survey of data provenancein 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. ofFAST, 2009, pp. 1–14.

[7] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: a tinyaggregation service for ad-hoc sensor networks," SIGOPS OperatingSystems Review, no. SI, Dec. 2002.

[8] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An efficient clusteringbased heuristic for data gathering and aggregation in sensornetworks," in Proc. of Wireless Communications and NetworkingConference, 2003, pp. 1948–1953.

[9] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanismto identify malicious packet dropping adversaries in sensornetworks," in Proc. of ICDCS Workshops, 2011, pp. 332–338.

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

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

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

Author's Profile:

Ms. Ayesha Firdous has completed her B.E in CSE Department from Bhojareddy Engineering College for women's. Presently she is pursuing her Masters in CSE from Shadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, India.

Ms. Sara Ali received the M.TECH degree from IIIT Bangalore and BE from Muffakham Jah College of Engineering and Technology. She is the Associate professor in the Department of Information Technology. She has 4 years of industrial Experience and 2 years of teaching experience.