International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Detecting Packet-Drops In Wireless Adhoc Networks Using Linear Authentication Based Approach.

1. Kyatham Sravanthi,2. Mrs P.Shylaja,3. V. Janaki
1.PG Scholar, Department of SE, Vaagdevi College of Engineering, Autonomous, Bollikunta, Warangal, Telangana.
Mail.id: sravanthi51.kyatham@gmail.com
2.Associate Professor, Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana.
Mail.id: pokalashylaja@gmail.com
3.Professor, HOD Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana.

ABSTRACT

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. In this paper, while observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. We are especially interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, we verify that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

INTRODUCTION

What is Mobile Computing?

Mobile computing is the discipline for creating an information management platform, which is free from spatial and temporal constraints. The freedom from these constraints allows its users to access and process desired information from anywhere in the space. The state of the user, static or mobile, does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away. Otherwise **Mobile computing** is a generic term used to refer to a variety of devices that allow people to access data and information from where ever they are.

Structure of mobile computing

Different types of devices used for the mobile computing:

1. Personal digital assistant/enterprise digital assistant
2. Smartphones
3. Tablet computers
4. Netbooks
5. Ultra-mobile PCs
6. Wearable computers
7. Palmtops/pocket computers

Applications of Mobile Computing:

1. Vehicles:

Tomorrow's cars will comprise many wireless communication systems and mobility aware applications. Music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB) with 1.5 M-bits/s. For personal communication, a global system for mobile communications (GSM) phone might be available offering voice and data connectivity with 384 k-bits/s. For remote areas satellite communication can be used, while the current position of the car is determined via global positioning system (GPS). Additionally, cars driving in the same area build a local ad-hoc network for fast information exchange in emergency situations or to help each other keeping a safe distance. In case of an accident, not only will the airbag be triggered, but also an emergency call to a service provider informing ambulance and police. Cars with this technology are already available. Future cars will also inform other cars about accidents via the ad hoc network to help them slow down in time, even before a driver can recognize the accident. Buses, trucks, and train are already transmitting maintenance and logistic information to their home base, which helps o improve organization (fleet management), and thus save time and money.

2. Emergency:

Just imagine the possibilities of an ambulance with a high quality wireless connection to a hospital. After an accident, vital information about injured persons can be sent to the hospital immediately. There, all necessary steps for this particular type of accident can be prepared or further specialists can be consulted for an early diagnosis. Furthermore, wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes.

3. Business:

Today's typical traveling salesman needs instant access to the company's database: to ensure that the files on his or her laptop reflect the actual state, to enable the company to keep track of all activities of their traveling employees, to keep databases consistent etc., with wireless access, the laptop can be turned into a true mobile office.

Benefits of Mobile Computing:

- Improve business productivity by streamlining interaction and taking advantage of immediate access

- Reduce business operations costs by increasing supply chain visibility, optimizing logistics and accelerating processes
- Strengthen customer relationships by creating more opportunities to connect, providing information at their fingertips when they need it most
- Gain competitive advantage by creating brand differentiation and expanding customer experience
- Improve business cycle processes by redesigning work flow to utilize mobile devices that interface with legacy applications

Advantages of Mobile Computing:

Mobile computing has changed the complete landscape of human being life. Following are the clear advantages of Mobile Computing:

1. Location flexibility:

This has enabled user to work from anywhere as long as there is a connection established. A user can work without being in a fixed position. Their mobility ensures that they are able to carry out numerous tasks at the same time perform their stated jobs.

2. Saves Time:

The time consumed or wasted by travelling from different locations or to the office and back, have been slashed. One can now access all the important documents and files over a secure channel or portal and work as if they were on their computer. It has enhanced telecommuting in many companies. This also reduces unnecessary expenses that might be incurred.

3. Enhanced Productivity:

Productive nature has been boosted by the fact that a worker can simply work efficiently and effectively from which ever location they see comfortable and suitable. Users are able to work with comfortable environments.

4. Ease of research:

Research has been made easier, since users will go to the field and search for facts and feed them back to the system. It has also made it easier for field officer and researchers to collect and feed data from wherever they without making unnecessary trip to and from the office to the field.

5. Entertainment:

Video and audio recordings can now be streamed on the go using mobile computing. It's easy to access a wide variety of movies,

educational and informative material. With the improvement and availability of high speed data connections at considerable costs, one is able to get all the entertainment they want as they browser the internet for streamed data. One can be able to watch news, movies, and documentaries among other entertainment offers over the internet. This was not such before mobile computing dawned on the computing world.

6. Streamlining of Business Processes:

Business processes are now easily available through secured connections. Basing on the factor of security, adequate measures have been put in place to ensure authentication and authorization of the user accessing those services. Some business functions can be run over secure links and also the sharing of information between business partners. Also it's worth noting that lengthy travelling has been reduced, since there is the use of voice and video conferencing.

EXISTING SYSTEM:

- The most of the related works preclude the ambiguity of the environment by assuming that malicious dropping is the only source of packet loss, so that there is no need to account for the impact of link errors. On the other hand, for the small number of works that differentiate between link errors and malicious packet drops, their detection algorithms usually require the number of maliciously-dropped packets to be significantly higher than link errors, in order to achieve an acceptable detection accuracy.
- Depending on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the related work can be classified into the following two categories.
- The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping.
- The second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

DISADVANTAGES OF EXISTING SYSTEM:

- In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attacker can camouflage under the background of harsh channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet

loss. This problem has not been well addressed in the existing system.

- In the existing system first category case, the impact of link errors is ignored.
- In the second Category, Certain knowledge of the wireless channel is necessary in this case.

PROPOSED SYSTEM:

❖ In this paper, we develop an accurate algorithm for detecting selective packet drops made by insider attackers.

❖ Our algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap—a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions.

❖ The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, by detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop.

❖ Our algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

ADVANTAGES OF PROPOSED SYSTEM:

✓ The proposed system with new HLA construction is collusion-proof.

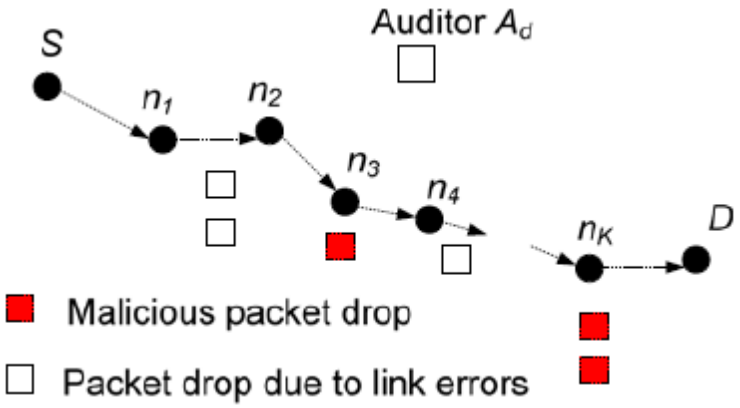
✓ The proposed system gives the advantage of privacy-preserving.

✓ Our construction incurs low communication and storage overheads at intermediate nodes. This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue.

✓ Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection. This mechanism allows one to trade detection accuracy for lower computation complexity.

SYSTEM ARCHITECTURE:

BLOCK DIAGRAM:



CONCLUSION

In this paper, we showed that compared with conventional detection algorithms that utilize only the distribution of the number of lost packets, exploiting the correlation between lost packets significantly improves the accuracy in detecting malicious packet drops. Such improvement is especially visible when the number of maliciously dropped packets is comparable with those caused by link errors. To correctly calculate the correlation between lost packets, it is critical to acquire truthful packet-loss information at individual nodes. We developed an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route. To reduce the computation overhead of the baseline construction, a packet-block-based mechanism was also proposed, which allows one to trade detection accuracy for lower computation complexity.

Some open issues remain to be explored in our future work. First, the proposed mechanisms are limited to static or quasi-static wireless ad hoc networks. Frequent changes on topology and link characteristics have not been considered. Extension to highly mobile environment will be studied in our future work. In addition, in this paper we have assumed that source and destination are truthful in following the established protocol because delivering packets end-to-end is in their interest. Misbehaving source and destination will be pursued in our future research. Moreover, in this paper, as a proof of concept, we mainly focused on showing the feasibility of the proposed cypto-primitives and how second order statistics of packet loss can be utilized to improve detection accuracy. As a first step in this direction, our analysis mainly emphasize the fundamental features of the problem, such as the untruthfulness nature of the attackers, the public verifiability of proofs, the privacy-preserving requirement for the auditing process, and the randomness of wireless channels and packet losses, but ignore the particular behavior of various protocols that may be used at different layers of the protocol stack. The implementation and optimization of the proposed mechanism under various particular protocols will be considered in our future studies.

REFERENCES

[1] J. N. Arauz, "802.11 Markov channel modeling," Ph.D. dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.

[2] 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.

[3] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

[4] 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.

[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] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.

[8] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

[9] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

[10] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia Antipolis, France, 2003.

[11] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193.

[12] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W.

Kellerer, “Castor: Scalable secure routing for ad hoc networks,” in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

AUTHOR’S DETAILS:

KYATHAM SRAVANTHI

PG Scholar, Department of SE, Vaagdevi College of Engineering, Autonomous, Bollikunta, Warangal, Telangana. Mail.id: **sravanthi51.kyatham@gmail.com**

Mrs P.SHYLAJA

Associate Professor, Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana.

Mail.id: **pokalashylaja@gmail.com**