International Journal of scientific research and management (IJSRM)
\||Volume||3||Issue||6||Pages|| 3094-3097||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Real-time Misbehavior Detection Approach By Prof Relay Node Formulation

Ms. Abirami.S [1], Dr. T. Senthil Prakash [2], Mr. Senthil.J, M.E.[3]

[1]PG Scholar, Department of CSE, Shree Venkateshwara Hi-TechEngg College,
Gobi, Tamilnadu, India,
abiramishanmugamn@gmail.com

[2]Professor & HOD, Department of CSE, Shree Venkateshwara Hi-TechEngg College,
Gobi, Tamilnadu, India,
jtyesp@yahoo.co.in

[3]Assistant Professor, Department of CSE, Shree Venkateshwara Hi-TechEngg College,
Gobi, Tamilnadu, India,
Senthilgobi05@gmail.com

Abstract: *Wireless sensor networks (WSNs) often consist of tiny devices and offer a variety of potential means to monitor the environment. WSNs are easily moved to several types of attack because of their use in critical applications, their distribution in open and unprotected environments and their limited system resources. Real-time backoff misbehaviour detector termed as the fair share detector (FS detector), is designed which exploits the non-parametric cumulative sum (CUSUM) test to quickly find a selfish malicious node without any a priori knowledge of the statistics of the selfish misbehavior. Based on the analytical model, it can compute the system configuration parameters for guaranteed performance in terms of average false positive rate, average detection delay and missed detection ratio under a perception delay constraint. The results to confirm the accuracy of our theoretical analysis as well as demonstrate the performance of the developed FS detector.*

Keywords: Selfish misbehaviour, real-time detection, FS detector, CUSUM test, Markov chain model**.**

1. Introduction

Wireless sensor networks have experienced an explosive growth during the past few years. Hacking issues are central concern for achieving secured communications in these networks. Wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physically to enhance the environmental setup such as temperature, sound, pressure, etc. and to co-operatively pass their data through the network to main location. The more contemporary networks are bi-directed, also enabling control of sensor activities. The execution of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as monitor the industrial processes and control, health monitoring by machine and so on.

To efficiently detect the backoff misbehavior, detection scheme needs to addresses the two main correlated challenges: 1) unknown misbehavior strategy, 2) real-time detection of the misbehavior. The first challenge has malicious node can be first behave as normal node and then manipulate its backoff timer to random small value at any time and we have no way to know the misbehavior strategy of A-priori. The second challenge has misbehavior needs to be detected in real time and then isolate the malicious node to prevent it from bringing more harm to the network as soon as possible. The existing solutions are cannot address the both issues at the same times [4], [5], [6], [7] or required modifications of the 802.11 protocols [8], [9].

In this paper, we develop an analytical model called G2G epidemic forwarding as an alternative to for the FS detector, which can provide quantitative performance analysis and theoretical guidance on system parameter configuration. Specifically, it has discrete-time Markov chain to model the behavior of the detector, because the detector's has next state depends only on its current values and the coming observation samples. This Markov chain-based model enables us to conduct rigorous quantitative analysis of the FS detector on three fundamental metrices: average of false definite rate, average of detection delays, and missed detection ratio and further compute the system configuration for guaranteed performances.

In particular, the Markov chain modeling contains the FS detector takes that different transition probabilities under the normal traffic conditions and also under the abnormal condition with misbehaving nodes respectively. The Nash equilibriums obtained from the normal traffic conditions can be used to directly calculate the average false positive rate and also provide the initial states for misbehavior analysis. Based on these initial states then use the Markov chain under the abnormal conditions to analyses the average detection delays and the missed detection ratios. Note that the missed detection ratio is not often considered in the context of the CUSUM test due to its "nonstop until detection" property. In this paper, we provide selfish node that is misbehavior detection by G2G policy.

2. Related Works

The problem of detecting backoff misbehavior over the 802.11-based medium access control (MAC) protocol has been widely studied in the literature. In [8], [9], modification of the 802.11 protocol is proposed to facilitate the misbehavior detection, where the receiver assigns a backoff timer for the sender. If the number of idle slots between consecutive transmissions from the sender does not comply with the assigned backoff timer, the receiver may label the sender as a selfish node. Modification to the 802.11 protocol and reliance on a trustworthy receiver are the main limitations of the work.

Another approach to deal with the backoff misbehavior is to develop protocols based on the game-theoretic techniques [14], [15], [16]. The goal is to encourage all the nodes to reach a Nash equilibrium. As a result, a malicious node is not able to gain an unfair share compared to well behaved nodes and, thus, discouraged from the misbehavior.

However, this category of approaches assumes that all the nodes are willing to deviate from the protocol when necessary, and the standard protocol needs to be modified. A heuristic sequence of conditions is proposed in [17], [18] to test multiple misbehavior options over the 802.11 MAC based on simple numerical comparisons.

This approach, named DOMINO, preserves its advantage of simplicity and easiness of implementation, and still demonstrates its efficiency when dealing with a wide range of 802.11 MAC misbehavior. However, the heuristic nature of the approach limits its applications to specific scenarios.

The sequential probability ratio test (SPRT) method is used in [5], [6], [7] to detect the 802.11 backoff misbehavior. The detection decision is made when a random walk of the likelihood ratio of observations (given two hypotheses)rises to be larger than an upper threshold. The main advantage of SPRT is that it can reach decision is very fast, given the complete knowledge of both normal behavior and backoff misbehavior strategy [20]. However, in arealistic setting, the strategy of malicious node is hard to know in advances. Furthermore, the existing work normally assumes that the backoff timer of each node is observable, which is again hard to achieve in practice because the transmission attempts involved in a collision are impossible to be distinguished. In our design, we monitor the successful transmission of the tagged node as the observation measurement.

The detection method in [3], [4] requires estimation of the collision probability of a packet transmitted. However, an inaccurate simplification there is to consider that packets from the misbehaving node and those from the normal nodes have the same collision probability. Such inaccuracy impacts both the performance of false positive rate and detection delay.

Furthermore, as a batch test method, the K-S statistic has its own drawback. Fixed-size data samples are needed to perform the test each time, which makes real-time detection difficult.

The detector in [19] directly counts the number of successful transmissions from a tagged node within an observation window1 to get a sample. Although such a sampling method is easy for implementation, the observation window needs to linearly increase with the number of nodes in the network to fairly count transmissions from each node, which as a result will increase the detection delay.

In this paper, we develop the new G2G detector, which takes every successful transmission over the network as a sample to trigger its state change. Such a sampling method is independent of the network size and turns out to result in good performance , as to be demonstrated later in this paper.

A common research issue among most of the existing schemes for misbehavior detection is their dependency on heuristic parameter configuration and experimental performances evaluation, which largely limit the flexibility and robustness of the schemes. To address this issue, in [19], we propose a Markov chain-based analytical model to theoretically analyze the detection performance and quantitatively configure the system parameters. In this paper, we develop the analytical model according to the newly proposed FS detector. Our analysis demonstrates performance improvement of the FS detector in real-time misbehavior detection over the original detector in [19].

3. System Design

As a distributed protocol, the DCF assumes that every node in the network operates in accordance with the standard to obtain a fair share of the wireless medium. Since there is nocentral controlling unit that assigns the backoff timer for each node, a malicious node can continuously choose a small backoff timer and then gain significant advantages in channel access probability over others. Moreover, because the increased transmission probability of the malicious node causes more collisions, normal nodes are forced to further exponentially defer their transmissions as they operate according to the protocol.

3.1 Create a Network

The windows are used to send a message from one to another. It creating the network each and every node will be having separate name and corresponding port number. Each node in the network will able to communicate with every node in the network.

3.2 Epidemic Forwarding

Every contact is used as an opportunity to forward messages. Node A meets Node B and A has a message that B does not have the message is relayed to node B. G2G Epidemic Forwarding is Nash equilibrium that is no self-indulgent node has a better choice than following the protocol truthfully. To protect the network against message droppers and against any other rational deviation.

3.3 Proof of Relay

The sender will check the proof of relay of the relay node while forwarding the message. The sender will check the relay regarding with the previous interactions between them. If the Relay Node responses correctly with the test message then only sender will send the data. The relay test phase message may contain encrypted type message.

3.4 Delegation Forwarding

Every node is associated with a forwarding quality that may depend on the destination of the message at stake. When a message is generated it is associated with the forwarding quality of the sender. A relay node A gets in contact with a possible further relay B, node A checks whether the forwarding quality of B is higher than the forwarding quality of the message. Node A creates a replica of the message, labels both messages with the forwarding quality of node B, and forwards one of the two replicas to B. Otherwise, the message is not forwarded.

3.5 Delegation Relay and Test Phase

The test by the sender is executed by the relay node as in G2G Epidemic Forwarding. Node A has an interest to send message via B. Node A asks B what it's forwarding quality to Destination D. Test phase the test by the sender is executed by the relay node as in G2G Epidemic Forwarding. This phase is used to find the forwarding quality if B Node in the network. That is B is not changing the message quality to get rid of the message quickly.

3.6 Detector design

We consider a saturated situation that a node always has data to send when the channel is available. Although a network in practice is not always saturated, the saturated scenario is of meaningful concern in the context of selfish misbehaving. If the network is lightly loaded, a misbehaving node will not impact much the throughput of normal ones. When the network is close to full utilization, the data buffer in every node have a very small probability to be empty, where the saturated model is a good approximation.

Let I = ¼ 0; 1; . . .g be the sequence of sample values of Iv, observed each time a successful transmission appears on the channel. Here, we drop the superscript v for easier presentation considering the clear context. There are N nodes and one access point (AP) in the network. Suppose that the initial value of the detector is X0 ¼ 0. If a successful transmission upon the nth observation is from the tagged node, i.e., In ¼ 1, the detector Xn increases by N _ 1; otherwise, In ¼ 0, and Xn decreases by 1 until it reaches 0.

The intuition of this design is as follows: In the normal situation, each node roughly takes turn to transmit; the increase of Xn caused by one successful transmission from the tagged node can then be equally offset by the successful transmissions from other N _ 1 nontagged nodes. Thus, the detector Xn will fluctuate around a low value close to zero in the normal situation. On the other hand, when the tagged node turns to misbehave and obtain more chances to transmit, it is not difficult to see that Xn is going to quickly accumulate to a large positive value.

The first aspect of inaccuracy in [3] is that the collision probability is estimated from only tens of samples, over which the variance may lead to overestimating the collision probability.

The behavior monitored by the detector is the idle time between consecutive successful transmissions; an overestimated collision probability will lead to an overestimated idle time (longer than its real value). With such an estimation error by the detector, a normal idle time observed will appear smaller than the normal behavior and, thus, misunderstood as misbehaving. That is, the overestimation of the collision probability leads to a higher false positive rate.

7. Conclusion

In this paper, we propose a novel fair share method called G2G epidemic forwarding in order to prevent from misbehaviors in Wireless Sensor Networks. Also, we develop a Markov chain based model to theoretically analyze the detection performance of the scheme. While most existing work for backoff misbehavior detection depends on heuristic parameter configuration and experimental performance evaluations are able to use our model for a quantitative study to achieve guaranteed detection performance in terms of average false definite rate, average detection delays and missed detection ratio. Moreover, we present simulation results that confirm the accuracy of our theocratical analysis and demonstrate the robustness of the FS detector. For our future work, we plan to systematically study the generic scenario with multiple misbehaving nodes in a multihop wireless network.

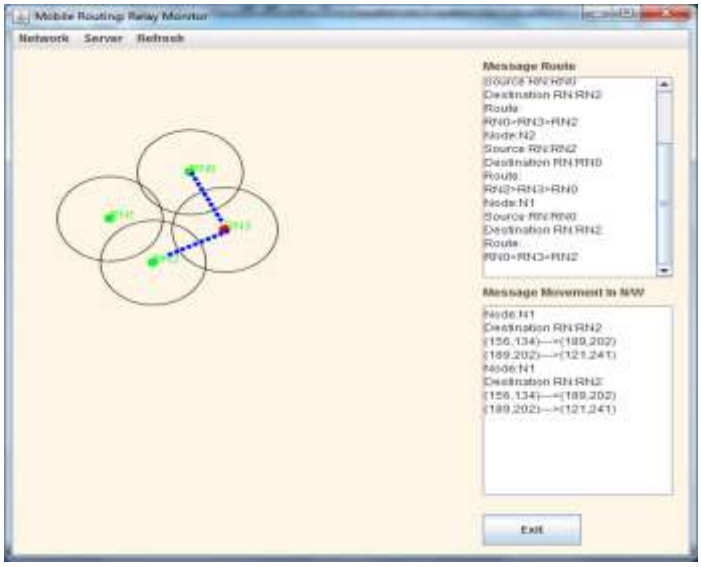

Figure 6.1 Status

References

[1] Jin Tang, Member, IEEE, Yu Cheng, Weihua Zhuang, "Real-Time Misbehavior Detection in IEEE 802.11-Based Wireless Networks: An Analytical Approach," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 1, JANUARY 2014no. 3, pp. 535-547, Mar. 2000.

[2] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," IEEE J. Selected Areas in Comm., vol. 18, no. 3, pp. 535-547, Mar. 2000.

[3] "MAD Wifi," http://www.madwifi.org, 2013.

[4] A. Toledo and X. Wang, "Robust Detection of Selfish Misbehavior in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 6, pp. 1124-1134, Aug. 2007. TANG ET AL.: REAL-TIME MISBEHAVIOR DETECTION IN IEEE 802.11-BASED WIRELESS NETWORKS: AN ANALYTICAL

[5] A. Toledo and X. Wang, "A Robust Kolmogorov-Smirnov Detector for Misbehavior in IEEE 802.11 DCF," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 1564-1569, 2007.

[6] S. Radosavac, J.S. Baras, and I. Koutsopoulos, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," Proc. ACM Workshop Wireless Security, pp. 33-42, 2005.

[7] S. Radosavac, G. Moustakides, J. Baras, and I. Koutsopoulos, "An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks," ACM Trans. Information and Systems Security, vol. 11, no. 4, article 19, July 2008.

[8] Y. Rong, S. Lee, and H. Choi, "Detecting Stations Cheating on Backoff Rules in 802.11 Networks Using Sequential Analysis," Proc. IEEE INFOCOM, pp. 1-13, 2006.

[9] P. Kyasanur and N. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," Proc. IEEE Int'l Conf. Dependable Systems and Networks (DSN '03), pp. 173-182, 2003.

[10] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 502-516, Sept./Oct. 2005.

[11] P. Serrano, A. Banchs, V. Targon, and J. Kukielka, "Detecting Selfish Configurations in 802.11 WLANs," IEEE Comm. Letters, vol. 14, no. 2, pp. 142-144, Feb. 2010.

[12] S. Szott, M. Natkaniec, and R. Canonico, "Detecting Backoff Misbehaviour in IEEE 802.11 EDCA," European Trans. Telecomm., vol. 22, no. 1, pp. 31-34, Jan. 2011.

[13] B. Brodsky and B. Darkhovsky, Nonparametric Methods in Change Point Problems. Kluwer Academic, 1993.

[14] C.E. Koksal, H. Kassab, and H. Balakrishnan, "An Analysis of Short-Term Fairness in Wireless Media Access Protocols," Proc. ACM Int'l Conf. Measurement Modeling Computer Systems (SIGMETRICS '00), 2000.

[15] M. Cagalj, S. Ganeriwal, I. Aad, and J. Hubaux, "On Cheating in CSMA/CA Ad Hoc Networks," Technical Report LCA - REPORT- 2004-017, EPFL, 2004.

Bibliography

Ms. Abirami. S, S.Abirami- Received the Bachelor Degree in Information Technology from Surya Engineering College in 2012. Currently she is doing Master of Engineering in Computer Science at Shree Venkateshwara Hi-Tech Engineering College under Anna University of India. Her research interests include Mobile computing and Network security.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E(CSE) degree from Vinayaka Mission's University, Salem, India in 2007 and M.Phil.,MCA.,B.Sc(CS) degrees from Bharathiyar University, Coimbatore India, in 2000,2003 and 2006 respectively, all in Computer Science and Engineering. He is a Member in ISTE New Delhi, India, IAENG, Hong Kong..IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 10+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17 International Journals, 43 International and National Conferences.

J.Senthil. B.E., M.E., (PhD, He is currently working as Assistant professor in IT department in Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamilnadu. His research interest includes Cloud computing and Cloud security.