IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks

S. Sathiyavani

Department of Computer Applications,Urumu Dhanalakshmi College, Trichy-620019

Available online at: www.ijcseonline.org

***Abstract* --**Mobile Ad hoc Networks (MANET) are self configuring, transportation less, dynamic wireless networks in which the nodes are resource constrained. Intrusion Detection Systems (IDS) are used in MANETs to monitor actions so as to detect any intrusion in the otherwise vulnerable network. In this paper, we present efficient schemes for analyzing and optimizing the time length for which the intrusion detection systems require to remain active in a mobile ad hoc network. A probabilistic model is proposed that makes use of help between IDSs among neighbourhood nodes to reduce their unit active time. Usually, an IDS has to run all the time on every join to oversee the network behaviour.

I. INTRODUCTION

Wireless sensor networks (WSN) are widely distributed autonomous sensors to observe physical parameters temperature, sound, pressure, etc. and to cooperatively pass their data throughout the network to a main location. The more modern networks are bi-directional; also enable control of sensor activity. The development of wireless sensor networks was enthused by military applications such as battlefield surveillance; today such network are used in many developed and consumer applications, such as industrial process monitor and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to some hundreds or even thousands, anywhere each node is connected to one (or sometimes several) sensors. every such sensor network node has typically several parts: a radio transceiver by means of an internal antenna or link to an outside antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, typically a battery or an embedded form of energy harvesting.

A mobile wireless sensor networks can just be defined as a wireless sensor network (WSN) in which the sensor nodes are transportable. MWSNs are a smaller, emerging field of research in difference to their well-established precursor. MWSNs are much more versatile than static sensor networks as they can be deployed in any situation and cope with rapid topology changes [1]. However, many of their application are similar, such as environment monitor or surveillance. The sensor nodes consists of a radio transceiver and a microcontroller powered by a battery, as well as several type of sensor used for effectively detecting light, heat, humidity, temperature etc.

A wireless sensor network (WSN) typically consists of a sink node now and then referred to as a base station in addition to a figure of small wireless sensor nodes. The base station is assumed to be secure with unlimited available power while the sensor nodes are supposed to be unsecured with limited available energy. The sensor nodes monitor an environmental area and collect sensory information. Sensory information is communicate [2] to the base position through wireless hop by hop transmissions. To conserve energy this information is aggregate at intermediate sensor nodes by applying a suitable aggregation function on the received data. Aggregation reduces the amount of system traffic which helps to reduce energy consumption on sensor nodes. It however complicate the already existing security challenges for wireless sensor network and requires new security techniques tailored specifically for this scenario. As long as security to aggregate data in wireless sensor networks is known as secure data aggregation in WSN. Were the first few works discussing technique for secure data aggregation in wireless sensor networks [3]. Two main security challenges in secure data aggregation are confidentiality and integrity of data.

II. RELATED WORK

[1] Anomaly recognition methods typically operate on pre-processed traffic traces. Firstly, mainly traffic capturing devices today employ random packet example, where each packet is selected with a certain probability, to cope with

increase link speeds. Secondly, temporal aggregation, where all packets in a dimension interval are represented by their temporal mean, is applied to change the traffic trace to the observation timescale of interest for anomaly detection. These pre-processing steps affect the chronological correlation structure of traffic that is used by anomaly detection method such as Kalman filtering or PCA, and have thus an impact on anomaly detection routine. Prior work has analyzed how packet sampling degrades the accuracy of irregularity detection methods; however, neither theoretical explanations nor solution to the sampling problem have been provided.

[2] In mobile ad hoc network, nodes have the inherent ability to move. Aside from conducting attacks to exploit their utility and cooperating with regular nodes to deceive them, spiteful nodes get better payoffs with the ability to stir. In this paper, we propose a game theoretic framework analyze the scheme profiles for regular and malicious nodes. We model the situation as a lively Bayesian signalling game and analyze and present the underlining link between nodes' best mixture of actions and the cost and gain of the individual scheme. usual nodes time following time update their beliefs based on the opponents' behaviour, while hateful nodes evaluate their risk of being caught to make a decision at what time to flee. Some possible countermeasures for normal nodes that can impact spiteful nodes' decisions are presented as well. An extensive analysis and imitation study shows that the planned equilibrium strategy summary outperforms other pure or mixed strategies and proves the importance of restricting malicious nodes' advantages bring by the flee option. jointly regular and hateful nodes' best responses are guided by threats about sure reactions from other players. Such threats are ward on their present beliefs. The regular node sets a reputation doorstep and judiciary other nodes' types based on the evaluated idea and this doorsill. The malevolent node continuously evaluates the risk, which is decided by the possibility that a regular node would want to report under current conditions. On the basis of the risk and expected flee cost, the malicious node makes a decision on fleeing. Moreover, mean nodes have the strategy of fleeing to avoid punishment in MANETs

[3] Traditional networks are built on the assumption that network entities cooperate based on a mandatory network message semantic to attain desirable qualities such as efficiency and scalability. Over the years, this statement has been eroded by the emergence of users that alter network behaviour in a way to advantage themselves at the expense of others. At one extreme, a mean user/node may eavesdrop on sensitive data or deliberately inject packets into the network to disturb authentication. In contrast network operations. The solution to this usually lies in encryption and, a rational node acts only to achieve an outcome that he requirements most. In such a case, cooperation is still achievable if the outcome is to the best attention of the node.

However, cooperation may be hard to uphold as it consumes scarce resources such as bandwidth, computational control, and battery power. This paper applies game theory to achieve collusive network behaviour in such network environments. In this paper, pricing, immoral listening, and mass punishments are avoided altogether. Our model builds on fresh work in the field of Economics on the theory of imperfect private monitor for the dynamic Bertrand oligopoly, and adapts it to the wireless multi hop system. The model derives conditions for collusive packet forwarding, truthful routing broadcast, and packet acknowledgments under a lossy wireless multi hop surroundings, thus capturing many important characteristics of the network coating and link layer in one integrated analysis that has not been achieved before. We also provide a proof of the viability of the model under a theoretical wireless setting. Finally, we show how the model can be applied to design a general protocol which we call the Selfishness Resilient Resource Reservation procedure, and validate the effectiveness of this protocol inside ensuring cooperation using simulations.

[4] We address issue related to establishing a defender's reputation in anomaly detection next to two types of attackers:1) smart insiders, who learn from historic attack and adapt their strategies to avoid detection/punishment, and 2) naïve attacker, who blindly launch their attacks without knowledge of the history. In this paper, we offer two novel algorithms for reputation establishment—one for system solely consisting of smart insiders and the other for systems in which both smart insiders and immature attackers is present. The theoretical analysis and routine evaluation show that our reputation-establishment algorithms can appreciably improve the performance of anomaly detection alongside insider attacks in terms of the trade off between uncovering and false positives. Our basic idea is for the defender to cautiously choose its strategy in the beginning to establish a desired reputation of hardiness (i.e., willingness to detect and punish attackers, even with a high cost of false alarms), which might force the upcoming attackers to drop their attacks and lead to a lower price in the long run. A typical

real-world example of this strategy is the police surge against criminal activities aimed at threatening potential criminals and reducing crimes further

[5] Due to the limited capability of sensor nodes in Wireless Sensor Networks (WSNs) in terms of calculation, communication, and energy, selecting the profitable discovery strategy for lowering resources consumption determines whether the IDS can be used almost. The signalling game is used to set up an interruption discovery game modelling the interactions between a malicious sensor node and an IDS agent, and its equilibrium are found for optimal detection strategy. Depending on the present belief, the best response strategy for the IDS agent can be gain based on the Perfect Bayesian equilibrium (PBE).The simulation results have shown the effectiveness of the future games, thus, the IDS agents are able to select optimal strategy to defend the spiteful sensor node's actions.

III. METHODOLOGY

Proposed Work

Cooperative game theory can be used to model situation in which players coordinate their strategies and share the payoffs flanked by them. The output of the game (individual payoffs that players receive) must be in balance so that no player has incentive to break away from the coalition. The game location in all the earlier game-theoretic work on IDS involves two sets of opposite players, the nodes/IDSs and the attacker/defaulters. In our proposed TRACEMOB, we have set a diversion that involves players (IDSs sitting in neighbouring nodes) cooperating to achieve a common goal (i.e., to monitor a single node). To the best of our knowledge, we have not come across any work on cooperating IDSs (to get a security versus energy trade off) that models such a situation using game theory. We have presented such a supportive multi-player game to model the interactions amid the IDSs in a neighbourhood and used it to validate our planned probabilistic scheme.

Background Process

This phase takes put right after route PSD is established, but prior to any data packets are transmitted over the route. In this phase, S decide on a symmetric-key crypto-system encrypt key; decrypt key and K symmetric keys key1; . . . ; key K, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S firmly distributes decrypt key and a symmetric key key j to node nj on PSD, for j ¼ 1; . . .;K. Key allocation may be based on the public-key crypto-system such as RSA: S encrypts key j using the community key of node nj and sends the cipher text to nj. nj decrypts the cipher text by its private key to obtain key j. S also announces two hash functions, H1 plus HMAC key , to all nodes in PSD. H1 is un keyed while HMAC key is a keyed hash purpose that will be used for message verification purposes later on. Besides symmetric key sharing, S also needs to set up its HLA keys.

ARCHITECTURE

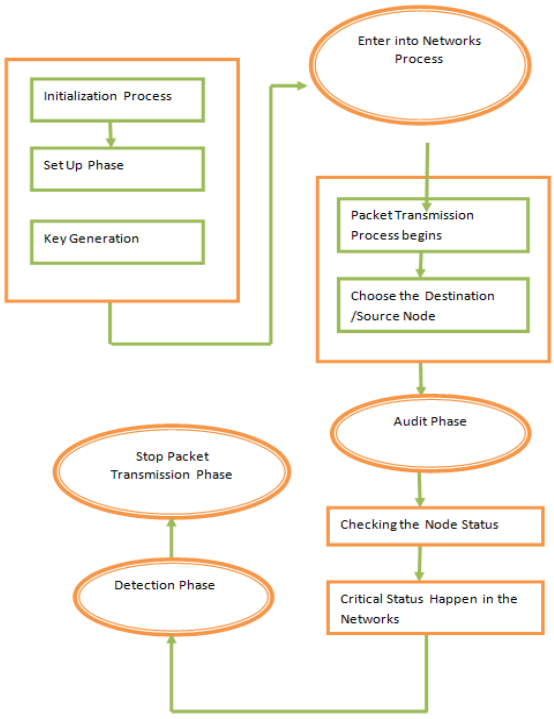


Fig1. Architecture

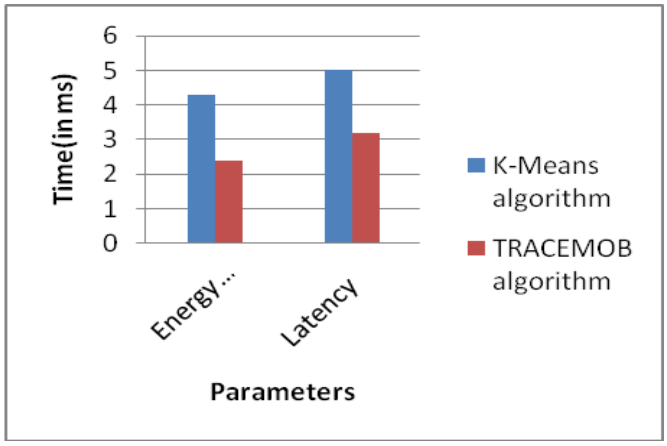
After finishing the setup phase, S enters the packet transmission phase. S transmits packets to PSD according to the following steps. Before distribution out a packet Pi, where i is a sequence number that exclusively identifies Pi, S computes and generate the HLA signature of ri for node nj, as follows the node has received, and it relays to the next hop on the direct. The last hop, i.e., node nK, only forwards Pi to the destination D. As prove in Theorem 4 in Section 4.3, the special structure of the one-way chained encryption building in (4) dictates that an upstream node on the route cannot get a copy of the HLA cross intended for a

downstream node, and thus the construction is elastic to the collusion model defined in Section 3.2. Note that here we think the verification of the integrity of Pi as an orthogonal problem to that of verify the tag tji. If the verification of Pi fails, node n1 should also stop forward the packet and should mark it accordingly in its proof-of-reception file

This phase is trigger when the public auditor Ad receives an ADR communication from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream course, i.e., n1; . . . ; nK, S's HLA public key information, the sequence information of the most recent M packets sent by S, and the sequence statistics of the subset of these M packets that were received by D. Recall that we assume the in sequence sent by S and D is truthful, because detecting attacks is in their attention. Ad conducts the auditing process as follows. Ad submits a random confront where the elements cji's are randomly chosen from Zp. Without loss of generality, let the series number of the packets recorded in the current proof-of-reception file be P1; . . . ; PM, with PM being the most recent packet sent by S. the above device only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reaction of a packet that it actually did not receive. This mechanism cannot avoid a node from overly stating its packet loss by claiming that it did not receive a packet that it really received.

The public assessor Ad enters the detection phase after receiving and auditing the reply to its confront from all nodes on PSD. The major tasks of Ad in this phase include the following: detecting any exaggeration of packet loss at each node, constructing a packet-loss bitmap for each hop, scheming the autocorrelation function for the packet loss on each hop, and decide whether malicious behaviour is present. Known the packet-reception bitmap at each node, b1; . . . ; ~b K, Ad first checks the constancy of the bitmaps for any possible overstatement of packet losses. Clearly, if to hand is no overstatement of packet loss, then the set of packets received at node j þ 1 have to be a subset of the packets received at node j. Because a normal node forever truthfully reports its packet reception, the packet reception bitmap of a malevolent node that overstates its packet loss must disagree with the bitmap of a widespread downstream node.

IV. EXPERIMENTS AND RESULTS



The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (a) keeping IDSs running throughout the simulation time and (b) using our proposed scheme to reduce the IDS's active time at each node in the network. From the simulation results, to observe that the effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. Here we have assumed a homogeneous network in a way that all the nodes have the same capacities in terms of their computational and energy resources.

V. CONCLUSION

An efficient way of using interruption detection systems (IDSs) that sits on every node of a mobile ad hoc system (MANET). We first present the minimization of the active period of the IDSs in the nodes of a MANET as an optimization trouble. We then described a cooperative game model to represent the connections between the IDSs in a neighbourhood of nodes. The game is defined in such a way that the main goal of the IDSs is to monitor the nodes in its neighbourhood at a desired safety level so as to notice any anomalous behaviour, whereas, the secondary goal of the IDSs is to conserve as a great deal energy as possible. To achieve these goals, each of the nodes has to contribute cooperatively in monitoring its neighbour nodes with a least amount probability. We then develop a distributed scheme to decide the ideal probability with which each node has to stay active (or switched on) so that all the nodes of the system are monitored with a desired security level. The assessment of the proposed scheme is done by comparing the performance

of the IDSs under two scenarios: (a) keeping IDSs running throughout the imitation time and (b) using our proposed scheme to reduce the IDS's active occasion at each node in the network.

REFERENCE

[1] S. Zeadally, R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, "*Vehicular ad hoc networks (VANETS): status, results, and challenges*," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.

[2] S. K. Bhoi and P. M. Khilar, "*Vehicular communication: a survey*", IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.

[3] S. Marti, T. J. Giuli, K. La and M. Baker, "*Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment*," Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255- 265, August 2000.

[4] C. Manikopoulos and L. Ling, "*Architecture of the Mobile Ad-hoc Network Security (MANS) System*," Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3122-3127, October 2003.

[5] K. Nadkarni and A. Mishra, "*Intrusion Detection in MANETs - The Second Wall of Defense*," Proc. IEEE Industrial Electronics Society Conference '2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.

[6] A. Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, "*Secure Routing and Intrusion Detection in Ad-hoc Networks*," Proc. 3rd IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March 8-12, 2005.

[7] N. Marchang and R. Datta, "*Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks*," IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.

[8] M. Hadded, R. Zagrouba, A. Laouiti, P. Muhlethaler, and L. A. Saidane, "*A multi-objective genetic algorithm-based adaptive weighted clustering protocol in vanet*," in Evolutionary Computation (CEC), 2015 IEEE Congress on, 2015, pp. 994–1002.

[9] Y. Peng, Z. Abichar, and J. M. Chang, "*Roadside-aided routing (RAR) in vehicular networks*," in IEEE International Conference on Communications, 2006, pp. 3602–3607.

[10] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "*Broadcast storm mitigation techniques in vehicular ad hoc networks*," IEEE Wireless Communications, vol. 14, no. 6, pp. 84–94, 2007.

[11] I. Tal and G.-M. Muntean, "*User-oriented cluster-based solution for multimedia content delivery over vanets*," in IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, 2012, pp. 1–5.

[12] Y. Shi, L. H. Zou, and S. Z. Chen, "*A mobility pattern aware clustering mechanism for mobile vehicular networks*," in Applied Mechanics and Materials, vol. 130, 2012, pp. 317–320.

[13] C. S. Jensen, D. Lin, and B. C. Ooi, "*Continuous Clustering of Moving Objects*," IEEE Transactions on Knowledge & Data Engineering, vol. 19, no. 9, pp. 1161–1174, 2007.

[14] J. Bernsen and D. Manivannan, "*Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification*," Pervasive and Mobile Computing, vol. 5, no. 1, pp. 1–18, 2009.

[15] K. Jagadeesh, S. S. Sathya, G. B. Laxmi, and B. B. Ramesh, "*A survey on routing protocols and its issues in vanet*," International Journal of Computer Applications, vol. 28, no. 4, pp. 38–44, 2011.

[16] S. Singh and S. Agrawal, "*Vanet routing protocols: Issues and challenges*," in Engineering and Computational Sciences (RAECS), 2014 Recent Advances in, 2014, pp. 1–5.

