Dynamic Routing Through Integrity and Delay Differentiated Routing to Control Energy Consumption and Attacks

B.J. Job Karuna Sagar[1], Dr. V. Kiran Kumar[2]
[1]Assistant Professor (Adhoc), Department of Computer Applications, Yogi Vemana University, Kadapa
[2]Associate Professor, Department of Computer Science, Dravidian University, Kuppam

Abstract

Wireless Sensor Network (WSN) is often outlined as a network of devices. Devices are denoted as nodes, which may sense the surrounding and communicate data gathered from the surrounding in wireless way. In WSN, the QoS requirements are delay, reliability, and throughput. Applications running on the same Wireless Sensor Network (WSN) they have different Quality of Services (QoS) Requirements. Mainly two requirements are low differed (delay) and high data integrity. These two requirements can't be satisfy at the same time. the idea of potential in physical science, we propose integrity and delay differentiated routing in Controlling Energy Consumption and Attacks, a multi-path dynamic routing algorithm. By constructing a virtual hybrid potential field, integrity and delay differentiated routing in Controlling Energy Consumption and Attacks separates packets of applications with different QoS requirements according to weight assigned to each packet, and routes them towards the sink through different paths to improve the data fidelity for integrity-sensitive applications and reduce end-to-end delay for delay-sensitive ones. Using proposed technique, we prove that integrity and delay differentiated routing in Controlling Energy Consumption and Attacks is stable. Simulation results demonstrate that integrity and delay differentiated routing in Controlling Energy Consumption and Attacks provides data integrity and delay differentiated services.

Keywords: *Wireless sensor networks, data integrity, delay differentiated services, dynamic routing, and potential field.*

I. INTRODUCTION

Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources. These sensor nodes can sense, measure, and gather information from environment and, some local decision process, they can transmit the sensed data to the user. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, power supply, radio, and an actuator.

WSNS, diversity and complexity of applications running over WSNs, the QoS guarantee in such networks gains increasing attention in research community. As a part of an information infrastructure, WSNs support various applications over same platform. Different applications have different QoS requirements. For instance, in a fire monitoring application, the event of a fire alarm should be reported to the sink as soon as possible. On the other hand, some applications require most of their packets to successfully arrive at the sink irrespective of when they arrive. For example, in habitat monitoring applications, the arrival of packets is allowed to have a delay, but the sink should receive most of the packets.

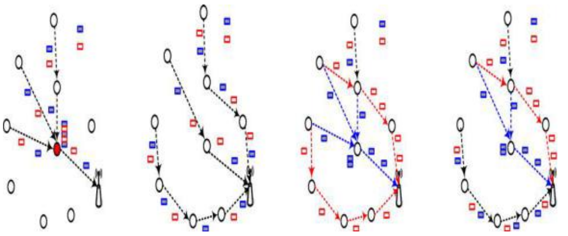

Figure 1: (a) Action of SPT. (b) Action of multipath router. (c) Action of integrity and delay differentiated routing in controlling Energy Consumption and Attacks. (c) integrity and delay differentiated routing in Controlling Energy Consumption and Attacks with hotspot

The QoS requirements can be application specific or network specific. For example, for the event tracking application QoS requirements can be coverage, optimum number of sensor that are need to be active, exposure etc. From network perspective, the QoS requirement can be maximum utilization of the sensors resources.

In WSNs, two basic QoS requirements are low delay and the high data integrity. In most of the situation these two requirements cannot be satisfied simultaneously. The paper mainly focus on how to design a routing protocol that provides data integrity and delay differentiated services over the same Wireless Sensor Networks even the network is congested.

II. LITERATURER SURVEY

1. “Modeling botnet propagation using time zones,”.
AUTHORS: D. Dagon, C. Zou, and W. Lee

Time zones play an important role in malware epidemics. We studied botnets, or coordinated collections of victim machines (zombies) controlled by attackers. Over a six month period we observed dozens of botnets representing millions of victims. We noted diurnal properties in botnet activity, which we suspect occurs because victims turn their computers off at night. Through binary analysis, we confirmed some botnets demonstrated a bias in infecting regional populations. Clearly, computers that are offline are not infectious, and any regional bias in infections affect the overall growth of the botnet. We created a diurnal propagation model. The model uses diurnal shaping functions to capture regional variations in online vulnerable populations. The diurnal models compare propagation rates for different botnets, and prioritize response. Because of variations in release times and diurnal shaping functions particular to an infection, botnets released later actually surpass other botnets that have an advanced start. Since response times for malware outbreaks is in hours, being able to predict short-term propagation dynamics to allocate resources. We used empirical data from botnets to evaluate the analytical model.

2. “Dissecting android malware: Characterization and evolution,”. AUTHORS: Y. Zhou and X. Jiang

The popularity and adoption of smart phones has greatly stimulated the spread of mobile malware, especially on Android. In light of their rapid growth, there is a need to develop effective solutions.
However, our defense capability constrained by the understanding of these emerging mobile malware and the lack of timely access to related samples. In this paper, we focus on Android platform and aim to systematize existing Android malware. More than one year effort, we managed to collect 1,200 malware samples cover the existing Android malware families, ranging from August 2010 to October 2011.Wesystematically characterize various aspects ,including installation methods, activation mechanisms, malicious payloads.

Based on the evaluation with four representative mobile security software, our experiments show best case detects 79.6% of them while worst case detects 20.2% in our dataset. These results clearly show better develop next-generation antimobile malware solutions.

3. “Protecting against network infections: A game theoretic perspective,”.
AUTHORS: J. Omic, A. Orda, and P. V. Mieghem
Security breaches and attacks are critical problems in today's networking. A key-point is that the security of each host depends not only protection strategies it chooses to adopt but also on those chosen by other hosts in the network.

The spread of Internet worms and viruses is only one example. This class of problems has two aspects. First, it deals with epidemic processes, and as such calls for the employment of epidemic theory. Second, the distributed and autonomous nature of decision-making in major classes of networks (e.g., P2P, ad- hoc, and most notably the Internet) call for the employment of game theoretical approaches. Accordingly, we propose a unified framework that combines N-intertwined, SIS epidemic model with a no cooperative game model. We determine the existence of Nash equilibrium of the respective game and characterize its properties. We show that its quality, in terms of overall network security, largely depends on the underlying topology. We then provide a bound on the level of system inefficiency due to the no cooperative behavior, namely, the "price of anarchy" of the game. We observe that the price of anarchy may be prohibitively high;
4. “Power laws, pareto distributions and zipf’s law,”.
AUTHORS: M. E. J. Newman,

When the probability of measuring a particular value of some quantity varies inversely as a power of that value, the quantity is said to follow a power law, also known variously as Zipf’s law or the Pareto distribution. Power laws appear in physics, biology, earth and planetary sciences, economics and finance, computer science, demography and the social sciences. For instance, the distributions of the sizes of cities, earthquakes, solar flares, moon craters, wars and people’s personal fortunes all appear to follow power laws. The origin of power-law behavior has been a topic of debate in the scientific community. Here we review some empirical evidence for the existence of power-law forms and the theories proposed to explain them.

III. RELATED WORK

So many algorithms improve the quality of service in wireless sensor networking. Algorithm may consider single QoS parameter or more than that. There are routing protocols like RAP, SPEED and EDF which are proposed to provide real-time service and Protocols like AFS, ReInforM and LIEMRO are proposed to improve the reliability.

The SPEED is QoS conscious protocol in WSN that ensures end to end QoS. Every individual hub holds the details of surrounding hubs and “Stateless Geographic Nondeterministic Forwarding (SNGF)” is used as a routing procedure to find the path. It manages selected shipping speed to all the packets. By dividing length to sink by speed an end to end delay is calculated. Last Mile course of action is used to provide communication service. Congestion can be minimized using this. However packet miss ratio is high when network is congested [3].

MMSPEED an extension of SPEED and this protocol provides multi route and multi speed for data. The QoS requirements like low delay and high data integrity are considered. Because of probabilistic multi-route packet forwarding, packet can select shipping speed. Routing is localized and allows different types of packet to go through network. By doing decision at each intermediate node it achieves both QoS requirements considered. But it consumes lot of power in doing so. The protocol suffers from wastage of the energy and data redundancy problem [4].

ReInForM, a routing algorithm which supplies wanted dependability at proportional cost. Protocol makes copies of the packet and transmits them through multiple paths. Reliability is achieved by doing this. ReInForM makes use of randomized forwarding mechanism which results in load balancing. But scares resources like energy and bandwidth usage is more and the global topology of the network should be known [6].

EQSR protocol for wireless sensor networks to recover from node failure. The protocol splits the traffic and routed through node disjoint paths across the network to achieve efficient load balancing. The real time and non real time queuing model is used to differentiate between real time and non-real time data traffic. “XOR-centered Forward Error Correction (FEC)” has been utilized to increase the reliability. But this protocol suffers from control overhead [7].

Hassanein, et al.,[10] proposed Reliable energy aware routing in wireless sensor networks. It mainly reduces energy wastage. The reliability is achieved by sending packets along multiple paths and acknowledgement. Source node initiates the routing procedure in this protocol. In the path discovery process packets are flooded by sink node.

The energy is reserved according to different energy requirement. It is used to reduce buffering and data loss in case of broken connection. This is not used under normal operation but used only when no path exist. End to end capability is minimized to capability of single path.

D. Djenouri and I. Balasingham, [14] proposed a localized QoS aware routing for Wireless Sensor Network. In network having different data traffic types, it is used to differentiating QoS essentials financial in accordance to the data type, which empowers to give diverse furthermore customized QoS metrics for per barter type. Among per bundle, the protocol undertakings to satisfy the compulsory information related QoS metrics during considering energy efficiency.

IV. PROPOSED WORK

There are various algorithms have been proposed to address the QoS requirements in WSN. The routing protocol can consider single QoS constraints or more. Due to the limited bandwidth and buffer size the existing system cannot consider two basic QoS parameters delay and data integrity. In the highly congested network these requirements cannot be satisfied simultaneously. So there is a need of new protocol for these parameters and should be scalable. [2] Jiao Zhang, et al., proposed on novel potential based routing protocol, integrity and delay differentiated routing to improve fidelity for data integrity applications and to decrease end to end delay for delay-sensitive applications. The data integrity packets are cached on under loaded path which suffers from large end to end delay where as delay sensitive packets will route through shortest path. It has following disadvantages. Energy consumption to transfer a packet is high. There can be routing loops. Data integrity can be destroyed by internal or external attacks.

To overcome the problems of existing system here integrity and delay differentiated routing in Controlling Energy Consumption and Attacks routing protocol is combined with LEACH protocol and homomorphic encryption. The basic step is to create potential field by calculating the potential depth for each node.

Clusters are formed by using LEACH which considers the energy and position. Based energy and potential depth value cluster head is selected for each cluster formed. Cluster head will be used to route the packets from one cluster to another until it reaches sink node. The packets are given weight which indicates the degree of delay sensitivity. Packets with zero weights are considered as data integrity packets and they are encrypted by using homomorphic encryption technique to maintain the integrity. Packets whose weights are not zero are delay sensitive packets which should travel shortest path to avoid end to end delay. The integrity and delay differentiated routing, potential based routing algorithm is used to differentiate different packets according to their weight and route them accordingly.

Energy consumption is minimized by using leach protocol. Security is provided by encrypting packets and has acceptable overhead.

This work aims to simultaneously improve the fidelity for high-integrity applications and decrease the end-to-end delay

for delay-sensitive ones, even when the network is congested. We borrow the concept of potential field from the physics and design a novel potential based routing algorithm, which is called integrity and delay differentiated routing . integrity and delay differentiated routing in Controlling Energy Consumption and Attacks is able to provide the following two functions: Improve fidelity for high-integrity applications. The basic idea is to find as much buffer space as possible from the idle and/or under-loaded paths to cache the excessive packets that might be dropped on the shortest path. Therefore, the first task is to find these idle and/or under loaded paths, then the second task is to cache the packets efficiently for subsequent transmission. integrity and delay differentiated routing in Controlling Energy Consumption and Attacks constructs a potential field according to the depth1 and queue length information to find the under-utilized paths. The packets with high integrity requirement will be forwarded to the next hop with smaller queue length. A mechanism called Implicit Hop-by-Hop Rate Control is designed to make packet caching more efficient. Decrease end-to-end delay for delay-sensitive applications. Each application is assigned a weight, which represents the degree of sensitivity to the delay. Through building local dynamic potential fields with different slopes according to the weight values carried by packets, integrity and delay differentiated routing in Controlling Energy Consumption and Attacks allows the packets with larger weight to choose shorter paths. In addition, integrity and delay differentiated routing in Controlling Energy Consumption and Attacks also employs the priority queue to decrease the queuing delay of delay-sensitive packets.

Advantages of Proposed System

1) integrity and delay differentiated routing in Controlling Energy Consumption and Attacks avoids the conflict between high integrity and low delay: the high-integrity packets are cached on the under loaded paths along which packets will suffer a large end-to-end delay because of more hops, and the delay-sensitive packets travel along shorter paths to approach the sink as soon as possible.

2) Using the Lyapunov drift theory, we prove that Integrity And Delay Differentiated Routing is stable.

3) Furthermore, the results of a series of simulations conducted on the TOSSIM platform demonstrate the efficiency and feasibility of the Integrity And Delay Differentiated Routing scheme.

V. METHODOLOGY

Service Provider

In this module, the service provider will browse the data file, initialize the router nodes and then send to the particular receivers. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver.

Router The Router manages a multiple networks to provide data storage service. In network n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and attacked nodes. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then router will connect to another node and send to particular user.

IDS Manager In this module, the IDS Controller consists of two phases. If Integrity or Malicious Data is occurs in router then IDS controller is activated. In a first phase DNS packets, Net flow, Traffic filter and Fine-grained IDS client detection are present. Aim is that detecting all hosts within the monitored network that engage in IDS communications. We analyze raw traffic collected at the edge of the monitored network and apply a pre-filtering step to discard network flows that are unlikely to be generated by IDS applications. We then analyze the remaining traffic and extract a number of statistical features to identify flows generated by IDS clients. In the second phase, Coarse-grained IDS Integrity or Malicious Data detection, Fine-grained IDS client detection and Integrity or Malicious Data are present; our system analyzes the traffic generated by the IDS clients and classifies them into either legitimate IDS clients or IDS Integrity or Malicious Data.

Receiver (End User) In this module, the receiver can receive the data file from the router. Service provider will send data file to router and router will send to particular receiver. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

Attacker Attacker is one who is injecting malicious data to the corresponding node and also attacker will change the bandwidth of the particular node. The attacker can inject fake bandwidth to the particular node. After attacking the nodes, bandwidth will have changed in a router.

VI. CONCLUSION

In this paper, a dynamic multipath routing algorithm Integrity And Delay Differentiated Routing is proposed based on the concept of potential in physics to satisfy the two different QoS requirements, high data fidelity and low end-to-end delay, over the same WSN simultaneously. The Integrity And Delay Differentiated Routing algorithm is proved stable using the Lyapunov drift theory. Moreover, the experiment results on a small test bed and the simulation results on TOSSIM demonstrate that Integrity And Delay Differentiated Routing can significantly improve the throughput of high-integrity applications and decrease the end-to-end delay of delay sensitive applications through scattering different packets from different applications spatially and temporally. Integrity And Delay Differentiated Routing provide good scalability because only local information is required, which simplifies the implementation. In addition, Integrity And Delay Differentiated Routing has acceptable communication overhead.

REFERENCE

[1] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: Accurate and scalable simulation of entire TinyOS applications," in Proc. 1st Int. Conf. Embedded Networked Sensor Syst., 2003, pp. 126–137.

[2] T. Chen, J. Tsai, and M. Gerla, "QoS routing performance in multi-hop multimedia wireless networks," in Proc. IEEE Int. Conf. Universal Personal Commun., 1997, pp. 557–561.

[3] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: Core extraction distributed ad hoc routing algorithm," IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1454–1465, Aug. 1999.

[4] S. Chen and K. Nahrstedt, "Distributed quality-of service routing in ad hoc networks," IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1488–1505, Aug. 1999.

[5] B. Hughes and V. Cahill, "Achieving real-time guarantees in mobile ad hoc wireless networks," in Proc. IEEE Real-Time Syst. Symp., 2003.

[6] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp. 738– 754, Jun. 2003.

[7] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, "RAP: A real-time communication architecture for large-scale wireless sensor networks," in Proc. IEEE 8th Real-Time Embedded Technol. Appl. Symp., 2002, pp. 55–66.

[8] M. Caccamo, L. Zhang, L. Sha, and G. Buttazzo, "An implicit prioritized access protocol for wireless sensor networks," in Proc. IEEE Real-Time Syst. Symp., 2002, pp. 39–48.

[9] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks," in Proc. IEEE 23rd Int. Conf. Distrib. Comput. Syst., 2003, pp. 46–55.

[10] P. T. A. Quang and D.-S. Kim, "Enhancing real-time delivery of gradient routing for industrial wireless sensor networks," IEEE Trans. Ind. Inform., vol. 8, no. 1, pp. 61–68, Feb. 2012.

[11] S. Bhatnagar, B. Deb, and B. Nath, "Service differentiation in sensor networks," in Proc. Int. Symp. Wireless Pers. Multimedia Commun., 2001.

[12] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: Reliable information forwarding using multiple paths in sensor networks," in Proc. IEEE Intl Conf. Local Comput. Netw., 2003, pp. 406–415.

[13] M. Radi, B. Dezfouli, K. A. Bakar, S. A. Razak, and M. A. Nematbakhsh, "Interference-aware multipath routing protocol for QoS improvement in event-driven wireless sensor networks," Tsinghua Sci. Technol., vol. 16, no. 5, pp. 475–490, 2011.

[14] J. Ben-Othman and B. Yahya, "Energy efficient and QoS based routing protocol for wireless sensor networks," J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 849–857, 2010.

[15] M. Razzaque, M. M. Alam, M. MAMUN-OR-RASHID, and C. S. Hong, "Multi-constrained QoS geographic routing for heterogeneous traffic in sensor networks, ieice transactions on communications," IEICE Trans. Commun., vol. 91B, no. 8, pp. 2589–2601, 2008.

[16] D. Djenouri and I. Balasingham, "Traffic differentiation-based modular qos localized routing for wireless sensor networks," IEEE Trans. Mobile Comput., vol. 10, no. 6, pp. 797–809, Jun. 2010.

[17] A. Basu, A. Lin, and S. Ramanathan, "Routing using potentials: A dynamic traffic-aware routing algorithm," in Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun. 2003, pp. 37–48.

[18] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: Congestion detection and avoidance in sensor networks," in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst., 2003, pp. 266–279.

[19] L. Georgiadis, M. J. Neely and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," Found. Trends Netw. vol. 1, no. 1, pp. 1–144, 2006.

[20] A. Papadoulos and J. A. Mccann, "Towards the design of an energy-efficient, location-aware routing protocol for mobile, ad-hoc sensor networkFs," in Proc. Int. Workshop Database Expert Syst. Appl., 2004, pp. 705–709.