IMPROVEMENT OF SECURITY AND EFFICIENCY IN INTERNET OF THINGS USING COGNITIVE LAYER

[1]K. Ravikumar, [2]S. RAMESH PRAKASH,

[1]Asst.professor, Dept.of.Computer science, Tamil University (Established by the Govt.of.Tamilnadu), Thanjavur-613010.

[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

ABSTRACT

The Internet of Things is a term describing a system of connected people, devices and services. Due to limited resources and scalability the security protocols for the Internet of Things need to be light-weighted. The cryptographic solutions are not feasible to apply on small and low energy devices of IoT because of their energy and space limitations. A light weighted protocol to secure the data and achieving data provenance is presented for the multi-hop IoT network. A solution modeled on human use of context and cognition, leveraging cloud resources to facilitate IoT on constrained devices. An architecture applying process knowledge to provide security through abstraction and privacy through remote data fusion . The data proxy uses the system models digitally mirror objects with minimal input data while the cognitive layer applies models to monitor the systems evolution and to stimulate the impact of commands prior to execution. The data proxy allows a system's sensor to be sampled to meet a specified quality of data system's sensor to be sampled to meet a specified quality of data target with minimal resource use. In this existing en-route filtering schemes are based on authentication. When a report is transmitted from a sensor node to the controller, each forwarding node checks whether the forwarding reports actually carry valid MACs. In proposed system we introduce a cognitive security layer means cognitive firewall for access the applications. In the cognitive firewall we send the command input and the Cognitive layer verify the data proxy and the Cognitive supervisor approved the valid commands input then only we access the application otherwise we can't access the applications.

Keywords: Internet of Things, security issues in IoT; security; privacy.

I. INTRODUCTION

The Internet is continuously changing and evolving. The main communication form of present Internet is human-human. The Internet of Things (IoT) can be considered as the future evaluation of the Internet that realizes machine-to-machine (M2M) learning. Thus, IoT provides connectivity for everyone and everything. The IoT embeds some intelligence in Internet-connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services. This paper addresses the existing development trends, the generic architecture of IoT, its distinguishing features and possible future applications. This paper also forecast the key challenges associated with the development of IoT. The IoT is getting increasing popularity for academia, industry as well as government that have the potential to bring significant personal, professional and economic benefits.

A router acts like a coin sorting machine, allowing only authorized machines to connect to other computer systems. Most routers also keep log files about the local network activity. In computer networking a routing table, or routing information base (RIB), is a data table stored in a router or a network host that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

The construction of routing tables is the primary goal of routing protocols. Static routes are entries made in a routing table by non-automatic means and which are fixed rather than being the result of routing protocols and associated network topology discovery procedures.

A routing table is analogous to a distribution map in package delivery. Whenever a node needs to send data to another node on a network, it must first know where to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a route to the destination node. Each node needs to keep track of which way to deliver various packages of data, and for this it uses a routing table. A routing table is a database that keeps track of paths, like a map, and uses these to determine which way to forward traffic. Nodes can also share the contents of their routing table with other nodes.

With hop-by-hop routing, each routing table lists, for all reachable destinations, the address of the next device along the path to that destination: the next hop. Assuming that the routing tables are consistent, the simple algorithm of relaying packets to their destination's next hop thus suffices to deliver data anywhere in a network. Hop-by-hop is the fundamental characteristic of the IP Internetwork Layer and the OSI Network Layer.

The primary function of a router is to forward a packet toward its destination network, which is the destination IP address of the packet. To do this, a router needs to search the routing information stored in its routing table.

A routing table is a data file in RAM that is used to store route information about directly connected and remote networks. The routing table contains network/next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the "next hop" on the way to the final destination. The next hop association can also be the outgoing or exit interface to the final destination.

The network/exit-interface association can also represent the destination IP address of the IP packet. This association occurs on the router's directly connected networks.

A directly connected network is a network that is directly attached to one of the router interfaces. When a router interface is configured with an IP address and subnet mask, the interface becomes a host on that attached network. The network address and subnet mask of the interface, along with the interface type and number, are entered into the routing table as a directly connected network. When a router forwards a packet to a host, such as a web server, that host is on the same network as a router's directly connected network.

A remote network is a network that is not directly connected to the router. In other words, a remote network is a network that can only be reached by sending the packet to another router. Remote networks are added to the routing table using either a dynamic routing protocol or by configuring static routes. Dynamic routes are routes to remote networks that were learned automatically by the router, using a dynamic routing protocol. Static routes are routes to networks that a network administrator manually configured.

The simplest forwarding model—unicasting—involves a packet being relayed from link to link along a chain leading from the packet's source to its destination. However, other forwarding strategies are commonly used. Broadcasting requires a packet to be duplicated and copies sent on multiple links with the goal of delivering a copy to every device on the network. In practice, broadcast packets are not forwarded everywhere on a network, but only to devices within a broadcast domain, making broadcast a relative term. Less common than broadcasting, but perhaps of greater utility and theoretical significance, is multicasting, where a packet is selectively duplicated and copies delivered to each of a set of recipients.

Networking technologies tend to naturally support certain forwarding models. For example, fiber optics and copper cables run directly from one machine to another to form a natural unicast media – data transmitted at one end is received by only one machine at the other end. However, as illustrated in the diagrams, nodes can forward packets to create multicast or broadcast distributions from naturally unicast media.

EXISTING CONCEPT:-

- In Cyber-Physical Networked Systems (CPNS), the challenger can inject false measurements into the controller throughcompromised sensor nodes, which not only threaten the security of the system, but also consume networkresources. To deal with this issue, a number of en-route filtering schemes have been designed for wireless sensor networks.

TECHNIQUE DEFNITION:-

En-route filtering is a scheme by whichintermediate nodes confirm the authenticity of messages and filter them when those messages travel through the network. In this existing en-route filtering schemes are based on authentication. When a report is transmitted from a sensor node to the controller, each forwarding node checks whether the forwarding reports actually carry valid MACs.

PROPOSED CONCEPT:-

In the proposed system we implement A cognitive security layer means cognitive firewall for access the applications. In the cognitive firewall we send the command input and the Cognitive layer verify the data proxy and the Cognitive supervisor approved the valid commands input then only we access the application otherwise we can't access the applications. Cognitive Firewall verifies the valid commands and the cognitive supervisor allow the valid data to access the application.

TECHNIQUE DEFNITION:-

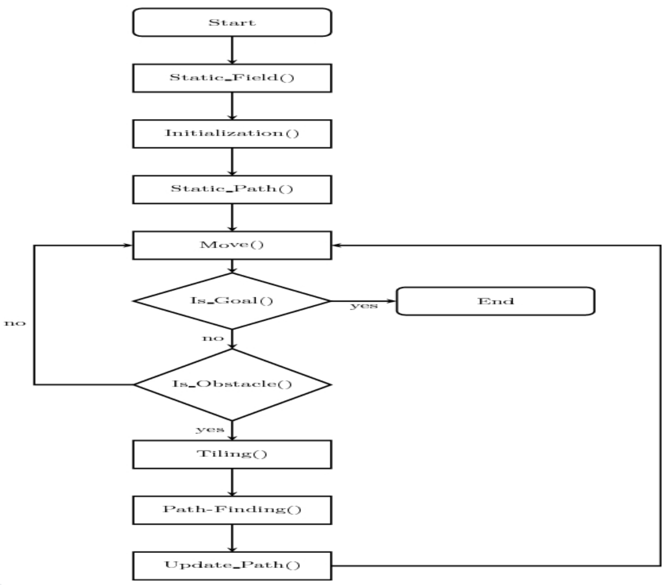
- A cognitive security layer means cognitive firewall for access the applications.
- In the cognitive firewall we send the command input and the Cognitive layer verify the data proxy and the Cognitive supervisor approved the valid commands input then only we access the application otherwise we can't access the applications.

Cognitive Firewall verifies the valid commands and the cognitive supervisor allow the valid data to access the application.

Connection establishment

To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

1. **SYN**: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.
2. **SYN-ACK**: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.
3. **ACK**: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.



Modules

- **Path Flow from Source to designation**
- **Shortest Path Finding**
- **Obstacle avoidance**

Path Flow from Source to designation

The main concept to determine shortest distance path and obstacle avoidance is providing user to reach at the destination with less time and with feasible path. It can predict as well as examine the shortest path from the number of paths. System can provide user-friendly interface for shortest path and obstacle .The user knows the source and destination address where he/she want to go, so by using this information our system will provide feasible solution.

A mechanism of our system that can reduces manpower and it can improve performance of system. The source and destination address is provide as a input to the system and with the help of that input whole process is carried out. A long distance and complex path we are providing to the system for increasing the performance of the system.

Shortest Path Finding

1) The motive of shortest path finding is to find feasible path from number of paths.

2) Shortest path problem defined for directed, undirected and mixed graphs.

In neural network this two models are available and are implementing these model simultaneously at a same time.

System, leverages path finding with the help of shortest path finding technique.

The motive is to predict feasible path with obstacle avoidance.

Obstacle avoidance

A modified algorithm called shortest path is presented for trajectory planning and obstacle avoidance. This method guarantees both smoothness and obstacle avoidance in the trajectories .The digital differential algorithm is used in this method to implement a linear and circular movement of robots and the Dijkstra's algorithm to search for the shortest path. Three simulation scenarios are used to implement this algorithm: The first one includes the building of a tree of paths between source and designation, the second one is for choosing the shortest distance from the source to target, and the third scenario is for comparison the length of the path and the time of arrival for different target designation.

CONCLUSIONS

Using the practical application of Usage Based Insurance, we demonstrated that Proxy models which are well calibrated to an underlying physical process may allow us to reduce the energy necessary to represent that process in the cloud. We demonstrated that querying information does not require one-to-one sampling of the sensors incrementing that process, and showed that it is possible to substantially minimize costs without significantly increasing measurement error. This level of abstraction and sensor fusion improves security by eliminating applications' direct access to physical systems and preventing the long-term storage of sensitive data. Further, this same technique may be used to minimize data transmitted, conserving costly bandwidth. This approach to cloud mirroring ultimately reduces technical, economic, and consumer sentiment barriers to the deployment of connective technologies. Ultimately, with the reduced bandwidth costs, computational requirements, and improved security facilitated by a context-aware, cognitive architecture for the Internet of Things, networking will become tenable on more devices in more places, helping to achieve the idealized vision of a fully connected network. Some challenges remain to be addressed. Model selection, for example, will remain an active domain of research, with a focus on characterizing and controlling for noise and model evolution. Other challenges relate more to system implementation - actuation latency and data accuracy may suffer due to the reduced sampling rate of Data Proxies, so research is needed to quantify the impact of these delays and accuracy losses. Relatedly, current data representations must be extended so that applications may account for the varied accuracy of information received in response to a request. A probabilistic extension to the Data Proxy may facilitate this accuracy reporting and ensure that returned data are sufficient to ensure a high degree of application performance. The Data Proxy's efficiency improvements will allow even the smallest, most resource-constrained device to join the ranks of "Big Data" systems, while this architecture's security improvements will enable new modalities for actuation never before possible. In the Data Proxy architecture, the Cognitive Layer protects the system against threats that manage to breach the Security Layer. The Cognitive Layer applies knowledge of the Data Proxy's model to identify and respond to a fault condition or to send notification to a secondary system or reviewer.

Future Enhancement

Future work will examine how best to define QoDs for various application types, how best to build and adapt Data Proxy models for a system in realtime, and how to quantify a Proxy's performance statistically. Additional work will focus on implementing a functional Cognitive Firewall to protect Smart Homes and Connected Cars, while the Cognitive Supervisor will be used to enable "Cognitive Prognostics" capable of identifying system faults early, reporting these automatically and providing rich information to aid in their repair. The use of this low-cost architecture will lead to the deployment of connected devices in more places, creating richer data mirrors and supporting enhanced pervasive sensing prognostic opportunities by reducing the amount of data needed to identify a fault. This architecture will also be adapted to work at the local network level, for example to apply an incar Cognitive Firewall and to reduce loading on constrained networks such the vehicle's Controller Area Network linking a vehicle's electronic control units. We further aim to extend this work from mirroring physical processes using sparse input data to include algorithmic processes dedicated to software monitoring, fault detection, and automated error correction in high-criticality systems that are not instrumented today. These systems include smart factories, infrastructure, and collaborative vehicle navigation systems. The cognitive elements of this architecture have the potential to transform how and what we connect to the Internet, affording greater opportunities and lower risks than conventional systems. This highly efficient and secure connectivity has the potential to transform all products with connected data in the design, manufacturing, and use phases.

REFERENCES

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 414–454, 2014. [2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/ pii/S0167739X13000241 [3] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [4] C. C. Aggarwal, N. Ashish, and A. Sheth, The Internet of Things: A Survey from the Data-Centric Perspective. Boston, MA: Springer US, 2013, pp. 383–428. [Online]. Available: http: //dx.doi.org/10.1007/978-1-4614-6309-2 12 [5] K. Bhaduri and M. Stolpe, Distributed Data Mining in Sensor Networks. Boston, MA: Springer US, 2013, pp. 211–236. [Online]. Available: http://dx.doi.org/10.1007/978-1-4614-6309-2 8 [6] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook," International Journal of Distributed Sensor Networks, vol. 12, no. 1, p. 7, 2016. [Online]. Available: http://dx.doi.org/10.1155/2016/3159805

[7] J. Siegel, "Data proxies, the cognitive layer, and application locality: Enablers of cloud-connected vehicles and next-generation internet of things," Ph.D. dissertation, Massachusetts Institute of Technology, Jun. 2016. [Online]. Available: http://hdl.handle.net/1721.1/104456

[8] V. Chang and M. Ramachandran, "Towards achieving data security with the cloud computing adoption framework," IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138–151, Jan. 2016. [9] L. Li, M. Rong, and G. Zhang, "An internet of things QoE evaluation method based on multiple linear regression analysis," in 2015 10th International Conference on Computer Science Education (ICCSE). IEEE, Jul. 2015, pp. 925–928. [10] E. Wilhelm, J. Siegel, S. Mayer, L. Sadamori, S. Dsouza, C.-K. K. Chau, and S. Sarma, "Cloudthink: a scalable secure platform for mirroring transportation systems in the cloud," Transport, vol. 30, no. 3, pp. 320– 329, 2015. [11] S. Mayer and J. Siegel, "Conversations with connected vehicles," in Internet of Things (IoT), 2015 5th International Conference on the. IEEE, Oct. 2015, pp. 38–44. [12] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," IEEE Transactions on MultiScale Computing Systems, vol. 1, no. 2, pp. 99–109, Apr. 2015. [13] M.-H. Maras, "Internet of things: security and privacy implications," International Data Privacy Law, vol. 5, no. 2, p. 99, 2015.

[14] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in 2014 IEEE Conference on Communications and Network Security. IEEE, Oct. 2014, pp. 79–84.

[15] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), ser. DAC '15, ACM. New York, NY, USA: ACM, Jun. 2015. [Online]. Available: http://doi.acm.org/10.1145/2744769.2747942

[16] J. Clover. (2016, Apr.) Macrumors. [Online]. Available: http://www.macrumors.com/2016/04/01/ belkin-wemo-homekit-compatibility-on-hold/

[17] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols,andapplications,"IEEE CommunicationsSurveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[18] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things," in Proceedings of the 14th ACM Workshop on Hot Topics in Networks, ser. HotNets-XIV, ACM. New York, NY, USA: ACM, 2015, pp. 5:1–5:7. [Online]. Available: http://doi.acm.org/10.1145/2834050.2834095

[19] S. Ratnasamy, D. Estrin, R. Govindan, B. Karp, S. Shenker, L. Yin, and F. Yu, "Data-centric storage in sensornets," Submitted to SIGCOMM, 2002.

[20] S. Adlakha, B. Sinopoli, and A. Goldsmith, "Optimal sensing rate for estimation over shared communication links," in American Control Conference, 2007. IEEE, Jul. 2007, pp. 5043–5045.

[21] L. Hu, Z. Zhang, F. Wang, and K. Zhao, "Optimization of the deployment of temperature nodes based on linear programing in the Internet of things," Tsinghua Science and Technology, vol. 18, no. 3, pp. 250–258, 2013.

[22] A. Jain, E. Y. Chang, and Y.-F. F. Wang, "Adaptive stream resource management using kalman filters," in Proceedings of the 2004 ACM SIGMOD international conference on Management of data, ser. SIGMOD '04, ACM.

New York, NY, USA: ACM, 2004, pp. 11–22. [Online]. Available: http://doi.acm.org/10.1145/1007568.1007573

[23] S. Li, L. Da Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and Internet of Things," IEEE Transactions on Industrial Informatics, vol. 9, no. 4, pp. 2177–2186, Nov. 2013. [24] A. Das and D. Kempe, "Sensor selection for minimizing worst-case prediction error," in International Conference on Information Processing in Sensor Networks, 2008. IEEE, Apr. 2008, pp. 97–108. [25] Z. Li, J. Ge, C. Li, H. Yang, H. Hu, B. Luo, and V. Chang, "Energy cost minimization with job security guarantee in Internet data center," Future Generation Computer Systems, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16307634

[26] C. D. Marsaon, "IAB Releases Guidelines for Internet-of-Things Developers," IETF Journal, vol. 11, no. 1, pp. 6–8, Jul. 2015.