TEDDI-B

TAMPER EVENT DETECTION
ON DISTRIBUTED INFRASTRUCTURE
USING BLOCKCHAIN

Abhishek Anand 2014103616
Prabhakaran S 2014103553
Sundar Vignesh J 2014103562

Guide
Dr. K. S. Easwarakumar

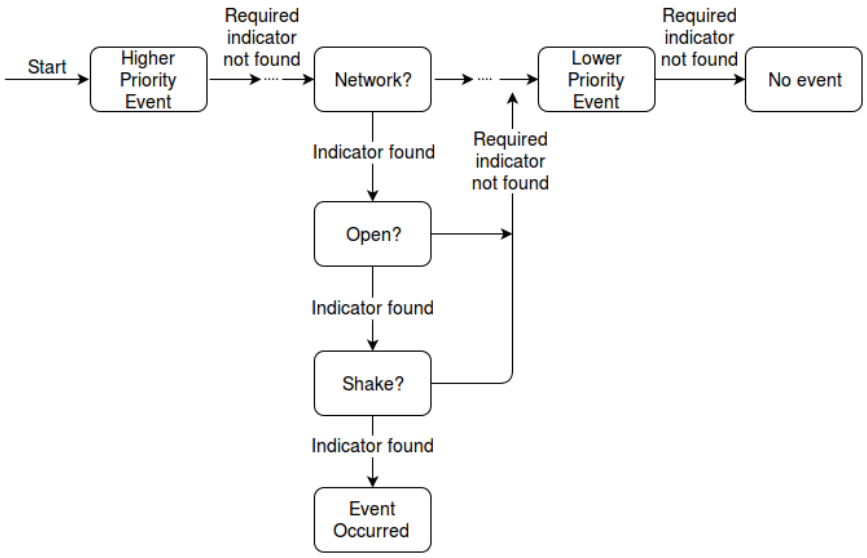
Signature

PROBLEM STATEMENT

Scada based edge devices such as power grids and water distribution control system provide automation and remote monitoring[1], present vulnerabilities[2] in a grid, as they are soft targets which may allow attackers access to critical assets in the network. They are vulnerable to physical damage and tampering. TEDDI is an existing system which solves the above mentioned problem using factor graph, however, it cannot handle Low & Slow Attack, Misordering Events.

RELATED WORK

TEDDI is an existing system for tamper protection using factor graph. It use factor graphs as our fusion algorithm for sensor data[3]. If a function is dependent on a variable, an edge is added to the graph between the nodes that represent this variable and function.Factor graphs allow for “arbitrary factorizations of joint distributions”[4], giving them the power to perform any task that a Bayesian network could while using a simpler model that can capture the defender’s intuition[5] about suspicious activity.

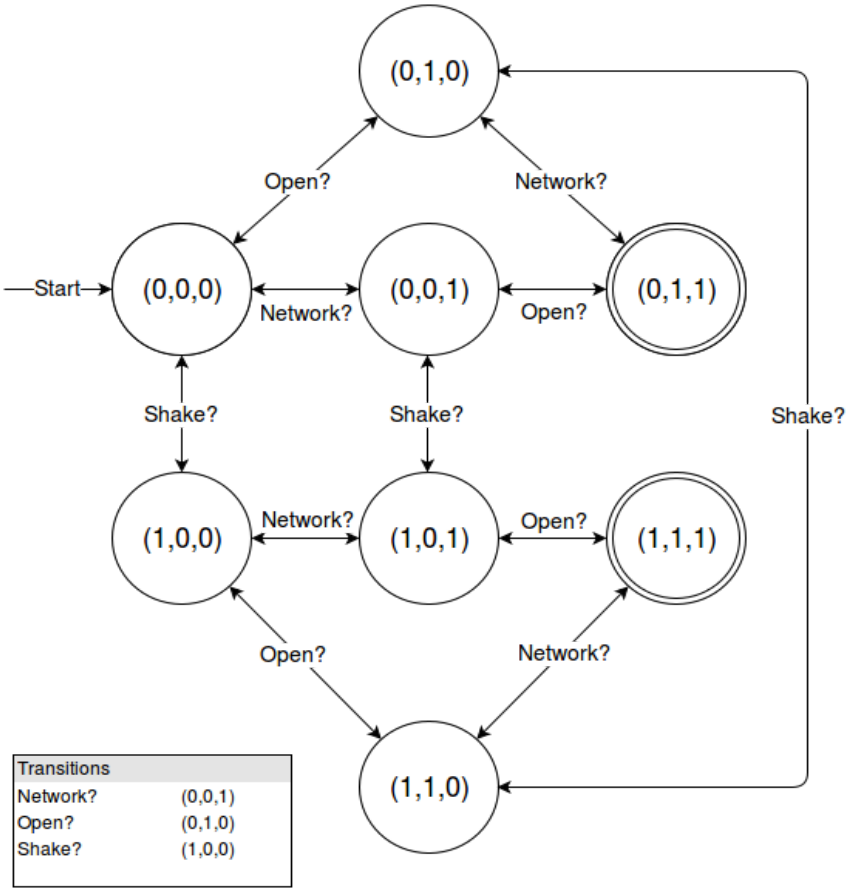


Blockchain in IoT

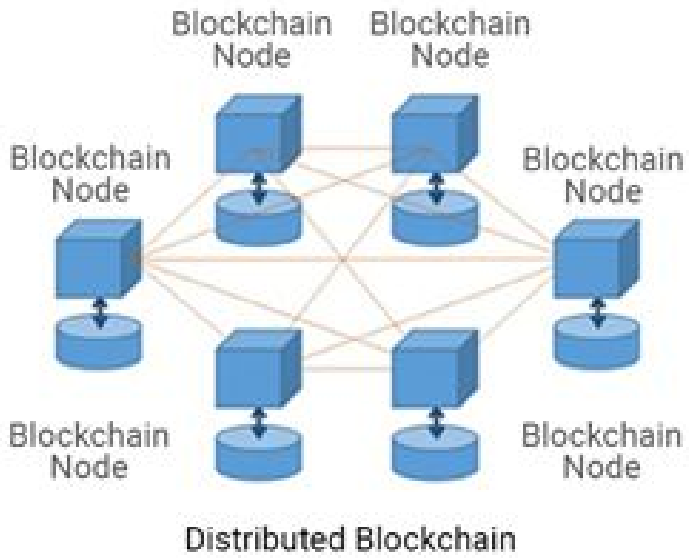
Blockchains allow us to have a distributed peer-to-peer network[where non-trusting IoT nodes can interact with each other without a trusted intermediary, in a verifiable manner. The blockchain-IoT combination is powerful and can cause significant transformations across several industries, paving the way for new business models and novel, distributed applications.

BLOCK DIAGRAMS

TEDDI-B deterministic finite automata



Introducing Block Chain in edge nodes



REFERENCES

[1] Boyer, Stuart A. *SCADA: Supervisory Control and Data Acquisition*. International Society of Automation, 2010.

[2] Igure, V., Laughter, S. and Williams, R. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7), pp.498-506.

[3] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, http://www.bitcoin.org

[4] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, submitted for publication.

[5] Abdalla, M., Boyen, X., Chevalier, C., Pointcheval, D.: Distributed Public-Key Cryptography from Weak Secrets. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 139–159. Springer, Heidelberg (2009)

[6] Jason Reeves and Sean W. Smith. Solving the grid defender's dilemma: Tamper pro- tection for distributed cyber-physical systems. In *The 12th International Conference on Security and Cryptography (SECRYPT)*, 2015.

[7] Jason Reeves and Sean W. Smith. Tamper event detection on distributed devices in critical infrastructure. In *The Second International Cryptographic Module Confer- ence (ICMC)*, 2014.
[8] Jason Reeves, Ashwin Ramaswamy, Michael Locasto, Sergey Bratus, and Sean W. Smith. Intrusion detection for resource-constrained embedded control systems in the power grid. *International Journal of Critical Infrastructure Protection*, 5(2):74–83, 2012.

OUTPUT

- Block chain designed using hyperledger.
- Bringing embedded devices in blockchain network.
- Bringing finite automata in edge devices