A Comparative Study On Authentication Protocols For IoT Devices

Author: Thomas Eckhardt, Supervisor: Miray Aysen, Responsible professor: Zekeriya Erkin, CSE3000 Research project June 2021
Contact details: t.eckhardt@student.tudelft.nl

Cyber Security Group
Department of Intelligent Systems
Delft University of Technology

1. Motivation

- Wireless Sensor Networks (WSN) are networks of wirelessly communicating sensors.
- Process, collect and communicate data back to the user [1]
- Use in environments such as vehicular polution level [2], wildlife [3], and healthcare monitoring [4].
- Set to grow from USD 3.282 million in 2018 to USD 8.669 million 2025 [5]
- Lack of adequate authentication is in top 3 vulnerabilities [6]
- For WSN's various lightweight authentication protocols have been introduced.

2. Sub-Questions

How do authentication protocols for Wireless Sensor Networks compare?

- How do these protocols compare in terms of performance?
- How do these protocols compare in terms of security?
- Where could improvements on these authentication protocols be made?

3. Method

Protocols that are compared in this study:

- **Wong et. al., 2006 [7]**
- **Vaidya et al., 2010 [3]**
- **Liu & Chung, 2017 [8]**
- **Gope & Hwang 2016 [4]**
- **Jiang et al., 2017 [9]**

- Literature study on authenication protocol for WSN's
- Comparison based on a performance and security analysis
- Find a gap where improvements could be made and suggest a solution

4. Results

Table 1: Performance of the registration phase

Name	Registration		
	User	GW node	Sensor node
Wong et al., 2006	T_{mes}	$3T_h + 2T_{\|\|} + T_{mes}$	-
Vaidya et al., 2010	T_{mes}	$3T_h + T_{\oplus} + T_{\|\|}$	-
Liu & Chung, 2017	T_{mes}	$T_{pu} + T_{pr}$	-
Gope & Hwang, 2016	$6T_h + 3T_{\oplus} + T_{mes}$	$5T_h + 3T_{\oplus} + 8T_{\|\|} + T_{mes}$	-
Jiang et al., 2017	$2T_h + 2T_{\|\|} + T_{mod} + T_{mes}$	$T_h + T_{\oplus} + 2T_{\|\|} + T_{mes}$	-

Table 2: Performance of the authentication phase

Name	Authentication		
	User	GW node	Sensor node
Wong et al., 2006	T_{mes}	$T_h + 2T_{\oplus} + T_{mes}$	$3T_h + 2T_{\oplus} + T_{\|\|} + 2T_{mes}$
Vaidya et al., 2010	$3T_h + T_{\oplus} + 4T_{\oplus} + T_{mes}$	$4T_h + T_{\oplus} + 8T_{\|\|} + T_{mes}$	$T_h + 3T_{\|\|} + T_{mes}$
Liu & Chung, 2017	$3T_{\|\|} + T_h + T_{\oplus} + T_{mes}$	$T_h + T_{\oplus} + T_{mes}$	$T_{\|\|} + 2T_h + 3T_{\oplus} + T_{mes}$
Gope & Hwang, 2016	$10T_h + 8T_{\oplus} + 15T_{\|\|} + T_{mes}$	$7T_h + 5T_{\oplus} + 11T_{\|\|} + 2T_{mes}$	$3T_h + T_{\oplus} + 4T_{\|\|} + T_{mes}$
Jiang et al., 2017	$5T_h + 2T_{\oplus} + 9T_{\|\|} + T_{mes}$	$8T_h + 2T_{\oplus} + 21T_{\|\|} + 2T_{mes}$	$6T_h + 4T_{\oplus} + 9T_{\|\|} + T_{mes}$

Table 3: Explanation of time notions

- T_h: Execution time for a one-way hash operation
- $T_{\oplus}$: Execution time for a xor operation
- $T_{||}$: Execution time for a concatenation operation
- T_{mes}: Execution time for sending a message

User: User of the system

Gateway Node (GW Node): Register new users and sensors. Sometimes referred to as Registration Center (RC)

Sensor Node: These are the nodes that collect, process and communicate the data.

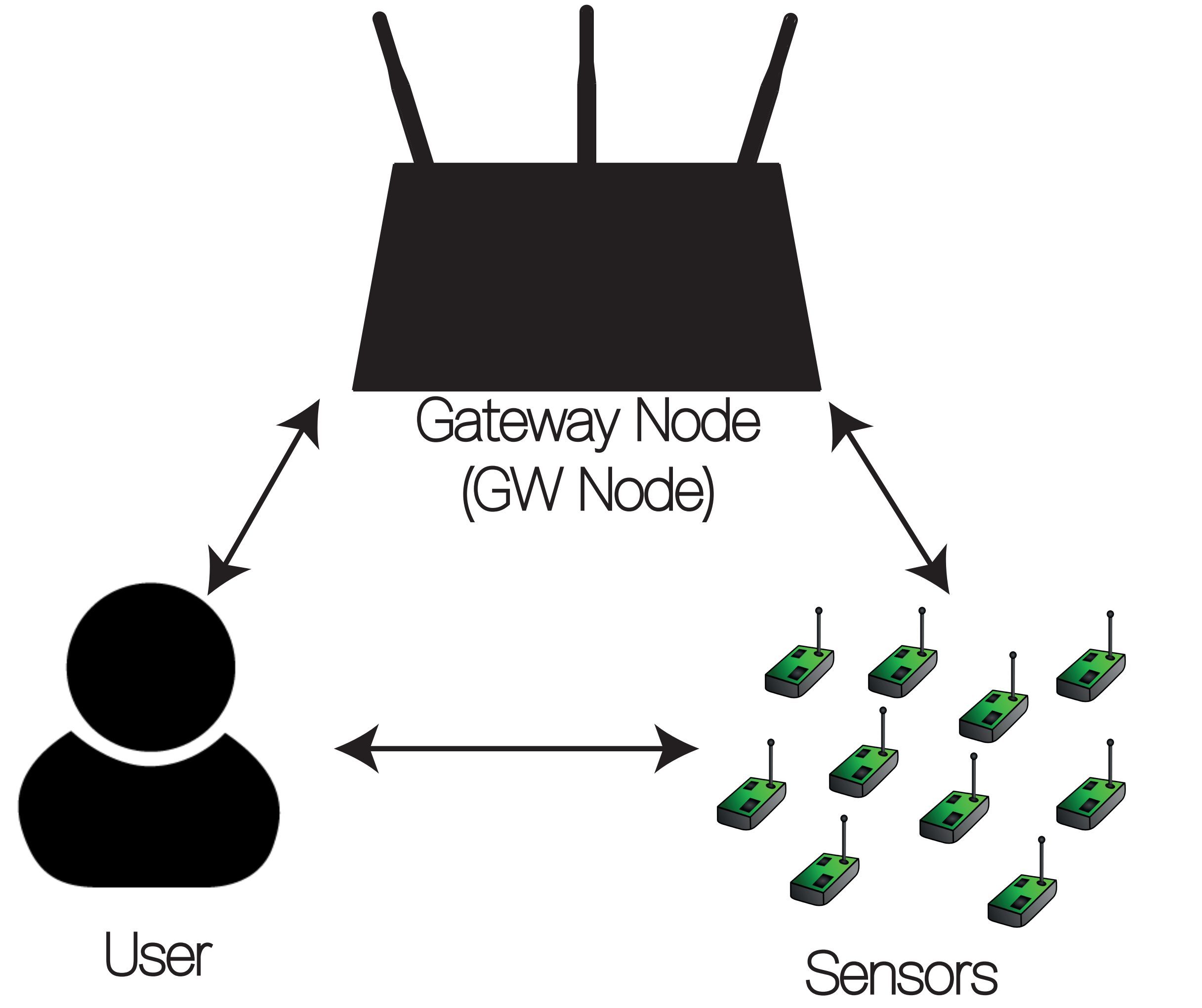
Table 3: Vulnerabilities of the authentication protocols

Attack types	Authentication protocols				
	Wong et al., 2006	Vaidya et al., 2010	Liu & Chung, 2017	Gope & Hwang, 2016	Jiang et al., 2017
Replay Attack	✘	✓	✓		
Impersonation Attack		✓	✓	✓	✓
Stolen-Verifier Attack	✘	✓	✓		
Guessing Attack		✓	✓		
Denial of Service Attack		✓	✓		✘
Node Compromise Attack		✓		✓	
Eavesdropping Attack					
Stolen Smart Card Attack				✓	✓
Tracking attack					✓
Forgery Attack	✘				
SID Modification Attack					✘

- It differ per protocol at which node most of the computation is done (User, GW and Sensor node).
- The sensor node are the most resource constrained, thus it would be benificial to move load away from these.
- Not all protocols are perfectly secure (e.g. Wong et al. and Jiang et al.)

5. Conclusion and Future work

- Improvements can be made by combining performance of one protocol, by the extra security features of other protocols.
- For the comparison the time notions could be translated to numbers, this could aid in comparing the protocols.



References

[1] Sanchez- Alvarez, D., Linaje, M., & Rodr ıguez-P erez, F. J.(2018). A framework to design the computational loaddistribution of wireless sensor networks in power con-sumption constrained environments.Sensors (Switzer-land),18(4). doi: 10.3390/s18040954

[2] Ullo, S. L., & Sinha, G. R. (2020). Advances in smartenvironment monitoring systems using iot and sen-sors.Sensors (Switzerland),20(11). doi: 10.3390/s20113113

[3] Vaidya, B., Makrakis, D., & Mouftah, H. T. (2010). Im-proved two-factor user authentication in wireless sen-sor networks.2010 IEEE 6th International Conferenceon Wireless and Mobile Computing, Networking andCommunications, WiMob'2010,8(3), 600–606. doi:10.1109/WIMOB.2010.5645004

[4] Gope, P., & Hwang, T. (2016). A Realistic LightweightAnonymous Authentication Protocol for SecuringReal-Time Application Data Access in Wireless Sen-sor Networks.IEEE Transactions on Industrial Elec-tronics,63(11), 7124–7132. doi: 10.1109/TIE.2016.2585081

[5] Grandviewresearch.(2018).Industrial wireless sensornetwork market size, sharetrends analysis reportby component (hardware, software, service), bytype, by technology, by application, by end use,and segment forecasts, 2019 - 2025.Retrievedfromhttps://www.grandviewresearch.com/industry-analysis/industrial-wireless-sensor-networks-iwsn-market

[6] OWASP. (2018).Owasp internet of things top 10 2018.Retrieved 2018, fromhttps://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[7] Wong, K. H., Yuan, Z., Jiannong, C., & Shengwei, W.(2006).A dynamic user authentication scheme forwireless sensor networks.Proceedings - IEEE Inter-national Conference on Sensor Networks, Ubiquitous,and Trustworthy Computing,2006 II, 244–251. doi:10.1109/SUTC.2006.1636182

[8] Liu, C. H., & Chung, Y. F. (2017). Secure user authenticationscheme for wireless healthcare sensor networks.Com-puters and Electrical Engineering,59, 250–261. doi:10.1016/j.compele-ceng.2016.01.002

[9] Jiang, Q., Kumar, N., Ma, J., Shen, J., He, D., & Chilamkurti,N. (2017). A privacy-aware two-factor authenticationprotocol based on elliptic curve cryptography for wire-less sensor networks.International Journal of NetworkManagement,27(3), 1–17. doi: 10.1002/nem.1937