Presented at 19th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Barcelona, Spain, September 2014.

Towards Secure Wireless TTEthernet for Industrial Process Automation Applications

Elena Lisova, Elisabeth Uhlemann[†], Johan Åkerberg, Mats Björkman
Mälardalen University, Västerås, Sweden
[†] Halmstad University, Halmstad, Sweden
{elena.lisova, elisabeth.uhlemann, johan.akerberg, mats.bjorkman}@mdh.se

Abstract — TTEthernet is a communication platform which builds on Ethernet, but extends it to include fault-tolerance and real-time mechanisms. The existing TTEthernet technology is developed for wired networks. A natural step for improving and extending the current application field is the introduction of a mixed wired and wireless network. However, this step requires research both about possible adaptation of existing systems as well as implementation of new technologies. A central research question is the security aspects of real-time sensor networks using wired and wireless technologies based on TTEthernet. In this paper, we identify and classify the most important aspects to consider in order to provide secure communications in such safety-critical industrial applications and propose a potential solution to address identified issues.

I. Introduction

Time-Triggered Ethernet (TTEthernet) [1] is a technology that allows extending Ethernet so that it can conform to applications where time-scheduling and predictability are the prime issues. To achieve this extension, several message traffic classes are used: Rate-Constrained (RC), Best-Effort (BE) and Time-Triggered (TT) traffic. TTEthernet allows partitioning all data into these different categories, all with different traffic policies and different temporal characteristics, such that safe and predictable communication for mixed-criticality systems can be established [1]. For instance, TT messages have the highest priority and therefore they are dispatched according to a predetermined schedule, and thus this traffic class is suitable for time-critical data. One significant TTEthernet feature is that it can be used for applications with different time and safety requirements. This way critical applications can coexist with best effort services without significant interference. Initially, TTEthernet was developed as wired system, but as more and more diverse application requirements emerge, there is a strong market need to make it mixed wireless and wired.

Wireless sensor networks have a number of evident advantages such as mobility, weight, size, simplicity and a list of others depending on the specific application. Hence, its implementation can increase the applicability area, especially in such domains as aerospace, automotive and industrial automation [2]. However, introducing wireless access also gives rise to new problems. Wireless links can more easily be intercepted and influenced as they open up communication also with intruders and eavesdroppers. Consequently, when considering a wireless version of TTEthernet for use in safety-critical applications with real-time requirements, security becomes a prime issue [2, 3]. A revised threat model is needed, the assets must be identified, and application specific security objectives should be defined.

When attempting to solve the problem of developing a secure wireless version of TTEthernet, existing standards and protocols for wired TTEthernet should first be considered [4]. Further, there are a number of wireless standards such as WiFi, WirelessHART and ZigBee, all of them with different security concepts and techniques. An analysis and comparison of these protocol standards can help developing a contemporary security framework that will reflect all necessary wireless features. In particular, we need to consider which threats that are specific for wireless systems; whether the assets set remains the same; which vulnerabilities that should be taken into account; and finally which changes should be introduced into the existing architectural concept for TTEthernet networks.

The main contribution in this paper is a detailed problem formulation targeting the development of a new security framework for mixed wireless and wired networks based on TTEthernet when used in industrial applications. In addition, we suggest a potential approach to solve the identified problems. The challenge that is especially addressed is achieving a standardized security framework that conforms to real-time demands, i.e. that the security mechanisms do not impact the real-time communication functionality, or else the remedy would itself become a denial-of-service attack [5].

The remainder of the paper is organized as follows. In Section II we consider the threat model by specifying the application requirements, the assets, the adversary goals and the adversary model. Section III presents an approach for defining essential system features that should be considered within possible security framework development. Section IV describes one possible solution namely Internet Protocol Security (IPSec), together with its drawbacks and ways of overcoming them. Finally, in Section V we represent our conclusions.

The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme FP7/2007-2013/ under REA grant agreement n°607727.

II. Threat Model

The threat model should reflect real adversary possibilities which are usually connected to the specific application, since this directly specifies the adversary goals, i.e., what an intruder targets, together with the assets that needs to be protected. Therefore the threat model should also include an adversary model. By adversary model we consider the specific features of an intruder, which can help understanding the possibilities of the intruder and structure ways to characterize the influence of an intrusion.

A. Applications Specification

We mainly target industrial applications due to their requirements on dependable transmission of real-time data. Nowadays sensor networks are widely used in industry for controlling, measuring and aggregation of data. For instance, a typical application example from process automation is a paper machine. To produce paper of required quality the humidity of the process should be measured continuously, as deviations from the specified values can lead to quality degradation. As a result real-time requirements are imposed by the system, and the humidity characteristic should be transmitted timely, reliable and continuously. Due to the speed of the paper production process, it is safer to measure humidity with wireless sensors rather than using a wired solution as wireless sensor can be fitted directly into a fast rotating part of the machine, rather than manually measuring using wired sensors.

B. Adversary Goals

The next step is setting the adversary goals and based on these, try to analyze what consequences it can have if the goals are reached and what countermeasures that can be imposed. According to [6], the three main adversary goals for sensor networks are disruption, eavesdropping and hijacking. As follows from the application example mentioned above, eavesdropping is not terminal for the considered sensor network. If an intruder can get information from the sensors (e.g. a water percentage in a specific type of paper) it can be objectionable as it potentially is a production secret but not fatal. On the other hand, if the intruder can change the data from the sensors or damage the system it may have terminal consequences. Therefore, eavesdropping can be eliminated from the list of adversary goals mentioned above. Consequently, the most significant adversary goals are disruption and hijacking as their impact on the targeted application is considerable.

C. Assets

When considering assets in applications with real-time constraints, one of the main assets is clock synchronization. Mazrahi provides a good classification of possible treats for clock synchronization in [7]: interception and modification; spoofing; replay; rogue master; interception and removal; delay manipulation; denial of service (DoS) attacks for OSI model layers 2 and 3; cryptographic performance; time source spoofing. This classification is very general and can be used regardless of if we consider a wired, wireless or mixed system. The specific set of tools needed to protect the asset clock synchronization depends on the system structure.

D. Adversary Model

In general, all adversary aspects mentioned in [8] are of importance for wireless TTEthernet applications. In particular, the most important adversary features in this context are: whether or not it is passive or active, static or adaptive, an insider or an outsider, the adversary mobility, communication capabilities and computational power.

A passive adversary is a prerequisite for an active one as at first, the adversary passively collects data and then, based on its analysis, starts to actively influence. If the adversary is an outsider, the goal is more connected to system disruption, as it is easier to suppress the channel or cause interference rather than to hijack the whole system. If the adversary is an adaptive one and can change its behavior depending on network response, it is more dangerous for the system functionality. Communication capabilities reflect whether the adversary acts through the network protocols or through the wireless channel or both. Possible adversary computational power depends on the specific application and the value of its assets. The higher the potential gain of interfering or hijacking a system, the more likely it is that the adversary invests in more computational power.

III. Approach

After defining the threat model we can propose an approach that includes a list of security objectives. By security objectives, we consider system features that should be imposed and according to which we can choose a protocol that can cover all, or almost all, requirements needed. Therefore we need to analyze the assets, i.e., the things we want to protect. We should identify in which way an adversary can gain possession of or control over the assets such that we can identify the objective of the security mechanisms that are introduced. The set of security objectives that should be introduced depends on the application (e.g. military or personal data). Initially, we consider all objectives mentioned in [8] and [9] and thereafter, we remove the ones that are not directly applicable for process automation applications.

Confidentiality. Generally this security objective refers to that the adversary must not know information from the sensors. However, according the identified adversary goals, confidentiality is not strictly required for considered application, as the level of paper humidity data is no secret, but rather a well-known fact used as a feedback to control the process.

Integrity. This notion is connected with the following questions: has the data been corrupted; can we trust this source? Integrity is a prime issue for the asset clock synchronization in applications with real-time constrains.

Authentication. By this we consider that we must know from whom (which network node) we get this information. Consequently, authentication is also a key point for the clock synchronization asset.

Availability. Mainly this objective refers to the fact that the service provided must be available, i.e., in our case, the paper making process must function all hours of the day since paper machines are too expensive to stand still. When considering our safety-critical application, availability is possibly the most important objective.

Anonymity. This notion usually is understood as the possibility to use a network without being identified or having private data shared without consent. As we consider sensor networks in process automation, this is not the most important security objective.

Auditability. System behavior reconstruction which is assured by auditability can help to enhance reliability if it is made adaptive, but if we are talking about safety-critical applications, it is not a prime issue as such systems should be as reliable as possible already from the beginning. Note that a sensor network used for controlling a paper machine can be considered safety-critical from the money loss point of view.

Nonrepudiability. This objectivity is about liability and has more legal than safety consequences, and therefore it is not a prime issue for the targeted application.

Third-party protection. This is about preventing damage done to third parties and it also more connected with reputation and legal consequences and therefore out of scope here.

Conformance. The network should work in accordance to the protocol. Just as with availability, this is one of the most important objectives for safety-critical applications.

After analyzing the security objectives mentioned above we can conclude that the ones that are most important for our considered applications are conformance, availability, integrity and authentication. Based on the list of identified objectives, we determine suitable techniques and approaches that can be used as a basis for the security framework. It is reasonable to first analyze existing protocols and techniques, to establish whether or not they can be of use for the identified set of targets above.

Two additional points also should be considered. Firstly, since TTEthernet is entirely compatible with Ethernet, we should evaluate protocols that can provide secure communications based on the Internet Protocol (IP). Secondly, we should look at the security analysis of wired TTEthernet [4], made by Steiner. The article provides some drawbacks and points to pay attention to in existing wired TTEthernet solution and also offers possible candidates for future developing. As shown in [4], systems based on TTEthernet can be vulnerable to internal attacks (e.g. replay attack). As possible security extensions replay protection, messages authentication and frame encryption are suggested.

IV. Potential Solution: IPSec

A possible candidate for the security framework of wireless TTEthernet is IPSec. IPSec [10] is a set of protocols which can provide the following types of protection: user data encryption, replay attack protection, and message integrity authentication. Devices in an IPSec network jointly decide which technique is needed according to their individual requirement specification.

The two main protocols that are used in IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP). The first one provides message integrity, data origin authentication and protection against replay attacks. The second one allows encrypting the whole datagram, using a set of encryption and authentication algorithms. Also one of the key points for IPSec is Internet Key Exchange (IKE). Mainly this is a combination of three protocol functions Internet Security Association (SA) and Key Management Protocol (ISAKMP) – a key exchange method; Secure Key Exchange Mechanism for Internet (SKEME) which provides public key encryption; and OAKLEY which contains specific key exchanging mechanisms for different key exchange modes. It is important to understand how IKE works, as the security objectives mentioned above only can be achieved only when this protocol is applied correctly.

All in all, IPSec provides a wide range of mechanisms for security which all depend on the specific combination of modes, IP versions and protocols. It complies with several of the above listed security objectivities. However, it also has several evident drawbacks. Firstly, IPSec is initially oriented towards point-to-point connections, so if used it in broadcast scenarios, adjustments are needed. Secondly, IPSec was not initially developed for application with real-time requirements. As these two problems appear as the two main showstoppers for relying only on IPSec as security protocol for mixed wireless and wired TTEthernet, the paper considers some suggestions on how to overcome them.

A. Solutions for Multicast

There exists some solutions for adapting IPSec to multicast mode, e.g., the Generic Route Encapsulation (GRE) protocol developed by Cisco. GRE is a tunneling protocol, which allows encapsulating protocols inside virtual point-to-point links over IP based internetworks using IPSec. Encapsulation in GRE can be performed on an arbitrary level, it is very general and allows a system that needs to transfer a packet to first encapsulate it in a GRE packet and next, this packet can again be encapsulated in yet another protocol and transferred through the GRE tunnel.

Another possible solution, also developed by Cisco, is called Dynamic Multipoint IPSec VPN (DMVPN), which can be described as a multipoint GRE (mGRE) together with the Next Hop Resolution Protocol (NHRP). NHRP is a protocol that dynamically can maps non-broadcast multi-access networks. Basically NHRP allows two functions, the first one is the possibility to allow a Next Hop Client dynamically registered with a Next Hop Server and the second one is the possibility for one client to dynamically find the mapping between the logical VPN IP and the physical IP of another client within the same network. Therefore when DMVPN is applied, IPSec is used as an encryption function, GRE or mGRE is used for setting up a tunnel and finally NHRP dynamically addresses different problems that may arise.

The techniques mentioned above can all be used for solving the IPSec multicast problem.

B. Solutions for Real-Time

When applying IPSec to TTEthernet, there are two main features that lead to problems with real-time requirements [11]. The first one is the increased packet size required by the additional IPSec headers and the second one is the time or complexity that must be spent on data encryption and decryption. There are several research results that show how the implementation of IPSec can affect the quality of service (QoS) characteristics of the systems [12], [13]. However, there are also several approaches available that can improve its QoS performance. IPSec performance can, for example, be improved by introducing the Multi-Layer IPSec (MLIPSec) protocol [14], which allows intermediate devices to decrypt parts of datagrams in order to speed up the routing process. However the possibility to use this method depends on the network size as well as its configuration and thus in some cases this approach is inapplicable. Furthermore MLIPSec is only suitable for static environments. Another approach, developed by Choi [15], is Mobile Multi-Layered IPSec (MML-IPSec). This approach includes an efficient key distribution protocol and also two mobile protocols. This technique is developed specifically for wireless communication and offers a dynamic version of MML-IPSec that allows varying security levels depending on data significance. The key distribution protocol includes mobility support, in the form of two protocols: Proactive Key Distribution (PKD) protocol and Dynamic Key Migration (DKM) protocol. The first one pre-establishes the SA with the current foreign agent and its neighbors, whereas the second one helps the SA to migrate between foreign agents while its user is moving.

It is important to note that increased packet size and increased delay due to encryption are features that mainly affect the delay in a predictable manner, which can be taken into account by the real-time scheduler. However, a fully loaded schedule may include task sets that are no longer schedulable if each packet requires more time to transmit and process. Alternatively, the overhead implied by IPSec may require longer time slots in a time-triggered setting which increases the overall superframe length. To determine if IPSec completely fulfills the real-time requirements of an existing sensor network, the network load should be estimated, which again will make its usefulness highly application specific. Also it is obvious that it is not enough to find a solution to each isolated problem, but also the combination of different protocols must be considered.

V. Conclusions and Future Work

In this paper, we have defined important aspects to consider when developing a security framework targeting applications based on wireless TTEthernet. As many of the solutions are rather application specific, we used process automation as a possible use case due to its inherent real-time requirements, the market drive to introduce wireless access technologies in industry and the need to be compliant with existing wired time-triggered networks. Based on this field of applications, we identified adversary goals, adversary models and system assets. In addition, we outlined an approach on how to address the identified issues, which includes a list of security objectives. Finally, IPSec was investigated as a possible solution, its drawbacks were listed and also different ways to overcome these drawbacks were proposed.

In future work we will further investigate how IPSec can be used for the security framework of wireless TTEthernet and how we can adapt and develop this protocol in accordance with the proposed techniques for real-time and multicast requirements.

References

[1] W. Steiner, G. Bauer, B. Hall, and M. Paulitsch, "TTEthernet: Time-Triggered Ethernet," in *Time-Triggered Communication*, R. Obermaisser, Ed., CRC Press, August 2011.

[2] Gundor, V.C. and G.P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *Industrial Electronics,* vol. 56, 10, p. 4258-4265, 2009.

[3] S. Raza, A. Slabbert, T. Voigt, and K. Landernas "Security considerations for the WirelessHart protocol," *in Proc. Emerging Technologies and Factory Automation*, Mallorca, Spain, September 2009, pp. 1-8.

[4] W. Steiner, "Candidate security solutions for TTEtnernet," *in Proc. Digital Avionics Systems Conference*, East Syracuse, NY, USA, October 2013, pp. 1-10.

[5] J. Akerberg, M. Gidlund, and M. Bjorkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," *in Proc. 9th IEEE International Conference on Industrial Informatics (INDIN)*, Caparica, Lisbon, July 2011, pp. 410-415.

[6] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Sensor network security: more interesting than you think" *in Proc. USENIX Workshop on Hot Topics in Security*, CA, USA, July 2006, pp. 5-5.

[7] T. Mizrahi, "Time Synchronization Security using IPsec and MACsec," *in Proc. 2011 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, Munich, Germany, September 2011, pp. 38-43.

[8] J.A. Clark, J. Murdoch, J.A. McDermid, S. Sen, H.R. Chivers, O. Worthington, and P. Rohatgi, "Threat modelling for mobile Ad Hoc and sensor networks," *in Proc. Second International Confrence on Internet Technologies and Applications*, Wrexham, Nort Wales, UK, September 2007, pp.25-27.

[9] D. Dzung, M. Naedele, T.P.V. Hoff, and M. Crevatin, "Security for Industrial Communication Systems," *PIEEE - Proceeding of the IEEE*, vol. 93, 6, pp. 1152-1177, 2005.

[10] S. Kent and S. Seo, *Security Architecture for Internet Protocol,* IETF RFC 4301, December 2005, http://www.rfc-editor.org/rfc/pdfrfc/rfc4301.txt.pdf

[11] R. Barbieri, D. Brusci, and E. Rosti, "Voice over IPsec: analysis and solutions," *in Proc. Computer Security Applications Conference*, Las Vegas, NV, USA, December 2002, pp. 261-270.

[12] B. Vaidya, J.W. Kim, J.Y. Pyun, J.A. Park, and S. Han, "Perfomance Analysis of Audio Streaming in Secure Wireless Access Network," *in Proc. International Conference on Computer and Information Science*, Jeju Island, South Korea, July 2005, pp. 556-561.

[13] O. Adeyinka, "Analysis of IPsec VPNs performance in a multimedia environment," *in Proc. International Conference on Intelligent Environments*, Seattle, WA, USA, July 2008, pp.1-5.

[14] Y. Zhang and B. Singh, "A multi-layer IPsec protocol" *in Proc. 9th USENIX Secutiry Symposium*, Denver, Colorado, August 2000, pp. 1-17.

[15] H. Choi, H. Song, G. Cao, and T.F.L. Porta, "Mobile Multi-layered IPsec," *Wireless Networks*, vol. 14, 6, pp. 895-913, 2008.