2017-08

Trust Integration for Security Optimisation in P2P-Based M2M Applications

Shala, B

10.1109/trustcom/bigdatase/icess.2017.335
2017 IEEE Trustcom/BigDataSE/ICESS
IEEE

Trust Integration for Security Optimisation in P2P-based M2M Applications

Besfort Shala, Patrick Wacht, Ulrich Trick, Armin Lehmann
Research Group for Telecommunication Networks
Frankfurt University of Applied Sciences
Frankfurt/M., Germany
shala@e-technik.org

Besfort Shala, Bogdan Ghita, Stavros Shiaeles
Centre for Security
Communications and Network Research
University of Plymouth
Plymouth, UK

***Abstract*—This publication presents a novel concept for securing P2P-based M2M applications using the integration of a trust management system. In addition, this publication presents different security problems inside the P2P-based M2M application (P2P4M2M) framework and evaluates P2P protocols based on security. Furthermore, this publication emphasises the importance of trust for ensuring security. This is done through a novel concept which uses special trust metric parameters for the P2P4M2M framework.**

Keywords— M2M; P2P; Service and Application; Security; Trust

I. INTRODUCTION

Machine-to-Machine (M2M) communications is applied in many different application fields, such as energy management, ambient assisted living, building surveillance, smart home, traffic management and electro mobility. These application fields aim to increase the quality of life and efficiency. The European Telecommunications Standards Institute (ETSI) defined M2M applications as "applications that run the service logic and use Service Capabilities accessible via open interfaces" [1]. There are different ways to realise service and application provision in M2M. The work and investigations of this publication are based on the P2P4M2M concept which offers new possibilities for applications, realised by several peers, independent of central instances or corporations [2] and the concept in [3] for testing P2P-based services and applications in M2M.

In [2] a framework that realises service and application provisioning using P2P networking in M2M application field is defined. A service, as well as an application, can be realised by peers using technical or non-technical principles. An application consists of one or more underlying services that are combined (i.e. aggregated or composed). These peers are represented by technical devices or humans who are networked using P2P mechanism. The use of the M2M community concept described in [2] forms a social network of peers and helps in avoiding legal restrictions, adjusting different interests among the peers and ensuring optimisation and forming P2P networks. The networking enables the participating peers to provide a service or an application that can be consumed by others [2]. According to [4], the information exchange between the peers for the service utilisation and the signalling to generate the application is enabled by using various M2M communication protocols (e.g., CoAP, HTTP, SIP, MQTT) based on SUBSCRIBE/ NOTIFY principle. The Service Management Framework (SMF) described in [5] is the main component for service and application provisioning in M2M based on the P2P4M2M framework [2]. Reference [5] introduces a Service Management Framework (SMF) installed in the local households, consisting of Service Delivery Platform (SDP) and Service Creation Environment (SCE), and uses the concept of P2P networked energy-community. The SCE brings the functionality to design and configure value-added services graphically compliant to the personal needs of the users [5]. Thus, the SMF used in the P2P4M2M framework gives every peer in the M2M community the possibility to create and configure M2M applications using the SCE which is integrated in the peer. Fig. 1 shows the structure of the P2P connected peers within an M2M community.

Reference [3] presents a concept for automated testing of decentralised services and applications in P2P4M2M. Also in [3] a testing framework with a special testing architecture for functional testing is introduced. The testing architecture is based on a global tester, called Test Master, and distributed testers, called Test Agents. Moreover, in order to deal with the increasing number of peers in the P2P4M2M framework, a Test Generation Environment is introduced. Fig. 2 shows the conceptual test architecture of the P2P4M2M framework.

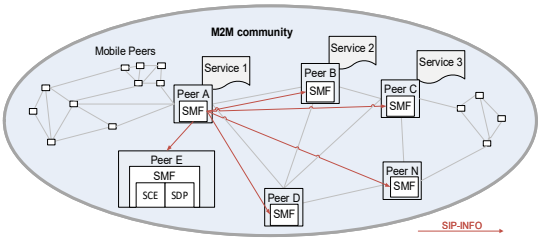

Fig. 1. P2P connected peers within a M2M community [2]

2324-9013/17 $31.00 © 2017 IEEE
DOI 10.1109/Trustcom/BigDataSE/ICESS.2017.335

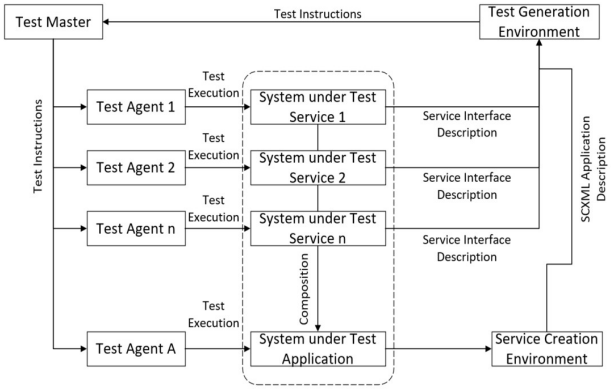

Fig. 2. Conceptual Test Architecture of the P2P4M2M framework

The two concepts presented in [2] and [3] lack the evaluation of different security issues in P2P4M2M and do not provide strategies to handle security risks. The increasing number of attacks in M2M networks creates the necessity to develop technologies for preventing attacks and system failures [9]. One aim of this publication is to define different security issues in P2P4M2M by evaluating security risks in P2P and M2M networks. In order to deal with the distributed nature of services and applications in [2], the testing architecture presented in [3] is modified and used for securing services and applications within the P2P4M2M framework. For ensuring security within the framework, the concept of trust and special trust metrics based on different evaluations are introduced.

In order to show the importance of this research work, this publication is structured into five sections. The introduction presents an overview about the concept of service and applications provisioning based on the P2P4M2M framework. Additionally, the concept and architecture of testing services and applications is presented. Section II evaluates the different security issues in P2P and M2M networks and defines security requirements. Section III presents the concept of trust and related work on trust. A novel concept for integrating a trust management system within the P2P4M2M framework is introduced in section IV and illustrated with an application example in section V.

II. Security Issues and Requirements in P2P4M2M

The P2P4M2M framework [2] has various challenges. Some of them were discussed in the past [2], however, security and the potential risks were not considered. Fig. 3 illustrates the functional architecture of the P2P4M2M framework which consists of several components and for security considerations the following general categorisation based on [4] can be made: a) M2M Network – includes M2M Application, M2M Service, M2M Communication Protocol, b) P2P Network – includes P2P Communication and P2P Overlay, c) IP Network. It has to be pointed out that there is a huge amount of publications dealing with IP networks and network security (e.g. [6] and [7]) which describe different vulnerabilities and several security solutions for IP Networks. However, the security for

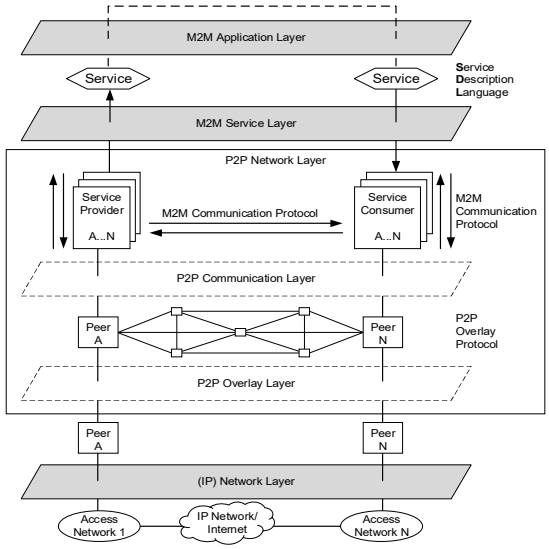

Fig. 3. Functional Architecture of the P2P4M2M framework [3]

the IP Network layer in this research is out of scope. This chapter describes the different security risks for M2M and P2P networks and shows a novel security comparison table of P2P protocols. Furthermore, it defines the security requirements for the P2P4M2M framework.

For M2M communications, [8] defines several potential security issues by dividing them in three categories: Physical attacks, logical attacks and data attacks. Also, [8] lists the different attacks for each category: Physical attacks include side channel attacks, software modification and malwares, destruction or theft of the M2M device. Logical attacks include impersonation, denial of service, relay attacks. Data attacks include privacy attacks, data modification and false information injection, selective forwarding/ interception. Furthermore, reference [9] provides an overview of the current state of security in sensor and ad-hoc networking for M2M communications. Exemplary for the application field of smart homes, [10] provides a landscape of threats assumed for smart home assets. Reference [8] states that M2M communications have to deal with all security issues of other network-based communications and [11] provides some security mechanisms including detecting the node compromise attack, lode location identifiers, two-way authentication and dual system.

P2P communication between the different services and applications plays a crucial role in P2P4M2M framework. According to [12] peer-to-peer (P2P) “is an instantiation of network architectures where all peers have equivalent authority and responsibility, differing completely from that of server and client system”. P2P overlays are virtual topologies that are built on top of physical networks. During the past years different P2P overlay protocols have been developed. The P2P overlay protocols used in P2P communications define different rules for communication in the overlay network, such as routing the messages over the overlay, bootstrapping into the overlay, mapping the nodes in the network and maintaining the nodes in the overlay. [2] mentions the different advantages in using P2P communication instead of client/ server architectures. Security

threats in P2P networks can be classified based on [12] in: eavesdropping, communication jamming, injection and modification of data, unauthorised access, repudiation, man-in-the-middle attack and sybil attack. Furthermore, based on several publications [13-23] the most relevant security attacks on different P2P protocols were derived and shown in Table I. Table I also shows a novel security comparison on different overlay protocols based on self-assessment, previously researches and publications [13-23]. Table I shows that most of the different P2P protocols are not secure against several security attacks and do not provide an efficient protection mechanism. Furthermore Table I shows that bootstrapping, Denial of Service (DoS) and identity attacks have the worst impact on security in the P2P overlay. Ensuring anonymity among the P2P nodes is also not solving the issue for most of the P2P protocols. The evaluation made in Table I concludes that the P2P protocol Freenet [22] mitigates best the different security attacks in comparison with other evaluated protocols and should be considered for further investigations.

Summarising the security issues for M2M and P2P networks described above and considering the nature of the P2P4M2M framework, two main categories of problems related to security can be identified: a) attacks from outside of the M2M community e.g. peers who want to harm the system by bootstrapping into the community. b) Attacks from the inside of the M2M community e.g. peers trying with a bad behaviour to break down by falsifying information in the community, network, or P2P layer. In order to successfully deal with these attacks, a security concept for preventing the entrance of malicious peers inside the community should be developed. The concept should also include a solution for preventing malicious behaviour of existing peers in the community. Peers and the services they use or provide play the most significant role in the P2P4M2M framework [2]. Based on [2] and Fig. 3, peers are using the P2P overlay for finding each other and for storing relevant information. Furthermore, they communicate using M2M communication protocols and are able to use and provide services. The different security issues described in [8] are executed by malicious peers and this is why the focus for ensuring security inside the P2P4M2M framework should be on peers. Due to different challenges stated above and based on [12], the following general security requirements can be defined: **Access control:** Protect against unauthorised access of peers. **Data integrity:** Ensure correctness of data provided by peers. **Data Confidentiality:** Protect data from unauthorised use. **User Authentication:** Prove the identity to a corresponding peer. **Non-Repudiation:** Prove the origin of data or peer. **Privacy:** Protect data from unauthorised view. **Anonymity:** Ensure anonymity of peers. In order to deal with the complexity and unique characteristics of the P2P4M2M framework and its security issues, the concept of trust has been introduced in the following chapter.

TABLE I. P2P OVERLAY SECURITY COMPARISON

Security issues	P2P Protocols								
	Chord	CAN	Tapestry	Pastry	Gnutella 0.4	Freenet	JXTA	Fast Track	Gnutella 0.6
Incorrect lookup routing	-	o	o	o	N	o	o	o	o
Incorrect routing updates	o	o	+	+	N	o	o	o	o
Incorrect forwarding	-	o	o	o	-	o	o	o	-
Sybil attacks	o	-	o	o	-	o	o	o	-
Eclipse attacks	o	-	o	o	-	o	o	o	-
Query hit attacks	N	N	N	N	-	N	o	o	o
Man in the middle attacks	-	o	o	o	o	o	o	o	o
Denial of Service attacks	-	-	o	-	-	o	o	o	o
Multiple joins and leaves	o	-	o	o	N	N	-	o	+
Invalid splits	N	-	N	N	N	N	N	N	N
Assigning node IDs attack	o	-	o	o	N	N	o	N	N
Bootstrap attacks	-	-	-	o	-	o	o	o	o
Virus injection	N	N	N	N	-	N	N	N	N
IP harvesting	N	N	N	N	-	o	N	N	N
Privacy	N	N	N	N	o	+	o	-	-
Anonymity	-	-	-	-	o	+	-	-	-

The following notations are used to assess the level of security: + high; - low; o medium; N not available.

III. CONCEPT OF TRUST AND RELATED WORK

As mentioned above, peers in the P2P4M4M framework [2] are connected P2P with each other and according to the evaluation made in Table I, attacks on the P2P layer can have a significant impact for the correct functionality of the whole system. Based on [24] it is difficult to implement security protections in P2P systems compared to centrally administered systems and security strategies need to be decentralised. Additionally, it is difficult to validate without centralised control peer identity and trustworthiness between peers [25]. Reference [25] also states that a P2P system relies on a set of distributed peers working fairly and properly together and defines the level of trust as "the level of confidence of one peer toward another peer with which it is communicating. As stated above on the basis of trust, many attacks can be mitigated by removing trustless peers from the system. This way, the existing peers are able to continue working reliably and providing trustworthy services without getting harmed by attackers. According to [26], trust can be defined as "an accumulated value from the history and the expecting value for the future. Trust is quantitatively/ qualitatively calculated and measured which is used to evaluate values of physical components, value chains among multiple stakeholder and human behaviours including decision making. Trust is broader concept that can cover security and privacy". Moreover, trust can be applied to peers providing a service and peers using a service. Furthermore, trust can be applied for provided services and applications. In this publication the focus is on applying trust to peers providing a service and the provided services. For evaluating trust, the following three main steps need to be accomplished: Data collection, data analysis and trust decision. For ensuring the collection of the right data, trust metrics need to be defined. [26] defines trust metric as "a measure to evaluate a level of trust by which a human or an object can be judged or decided from trustworthiness". Reference [26] also defines the concept of trust model as "a method to specify, build, evaluate and ensure trust relationships among entities".

Based on defined requirements the collected data has to be analysed and evaluated by the trust decision process – process for setting up the level of trust for the tested element.

There are several publications dealing with trust management systems in the M2M, Internet of Things (IoT) and P2P domain. A summary of the most relevant publications is presented as follows. Reference [27] proposes a distributed trust management system in combination with reinforcement learning for using in mobile M2M communications by utilising the history of node´s interactions to build trust among other nodes. This approach performs good results in terms of execution time and energy consumption. For evaluating trust between nodes [28] introduces a trust management model which uses information generated from direct communication with the node and allows nodes to be completely autonomous in the decision-making about the behaviour of other nodes in the IoT domain. In [29] a trust management scheme is presented where trust is evaluated based on both direct user satisfaction experiences of past interaction experiences and recommendations from others considering social relationships. A fuzzy-based approach for ensuring trustworthiness in IoT is proposed in [30] who defines network related trust metrics and also considers the energy consumptions for trust evaluation. The drawback of the approaches described above is that they do not consider the initial trust level of a peer and relay at the beginning on predefined trusted existing peers in the system. A different approach is provided by [31] who proposes a centralised trust management system with different trust management servers covering different geographical locations for trust computation. The problem of this solution is the single point of failure of the centralised system and the low level of usability in large scale systems. In [32] a reputation-based trust supporting framework, named PeerTrust, is introduced which includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. The disadvantage of this approach is that it does not consider the special characteristics of M2M systems and that it focuses only in P2P social communities, such as online markets. The main drawback of the trust management systems described in [27-32] is that they do not consider the different services a peer can provide and the trust level of the composed application based on the P2P4M2M framework. Moreover, they do not consider the trustworthiness of collected trust data of each peer.

IV. Requirements and Principles of Trust Management System in P2P4M2M

The aim of this research is to present a trust management system (TMS) which provides the possibility to provide secure trust evaluation considering the special characteristics of the P2P4M2M framework described in the introduction. The huge amount of data collected in the P2P4M2M should be processed and analysed in a trustworthy way. Based on the trust metric parameters and the results of the trust evaluation, the peers are categorised as either trustworthy or untrustworthy. For the trust management system presented in this research the following requirements were initially defined. To avoid centralised management and controlling, trust computing and evaluation have to be realised without any central authority, thus this process has to be **autonomous and decentralised**. For ensuring trust from the beginning of a working service, the **initial trust level of it** has to be considered and evaluated. This enables the possibility for the peers to figure out faster trustworthiness among other peers and services. The trust management system needs to ensure **flexibility** since one of the challenges in the P2P4M2M framework is the heterogeneity of peers and services. An important requirement is also the **volatility of peers and services.** In a P2P-based community, where a huge amount of peers are connected with each other without central authority, peers are able to suddenly enter or leave the network and this leads to rapid changes in existing trust relationships between peers. As the number of peers and services follows an increasing trend, the trust management has to ensure **scalability and stability.** Peers are able to provide more than one service and the trust evaluation must not be based only on one service but has to consider the **variety of different services** provided by the peer. Furthermore, the trust management system needs to consider **context-dependency** and to ensure that a peer can trust e.g. service 1 but mistrust service 2 of another peer**.** The trust computing and evaluating will generate a significant amount of trust data among the peers and the trust management system has to provide a mechanism for securing trust data storage and to ensure with that the **trustworthiness of trust data.**

As mentioned in the previous section, the concept of trust in this research is interpreted as a value for measuring the reliability and correctness of different working services provided by different peers and used in several composed applications. As any peer can provide many services within the P2P4M2M framework we consider that the total trust level of a peer consists of the trust levels the services it provides. For that reason, we focus on trust evaluation based on services. The architecture testing framework described in [3] is considered for the integration of a TMS. Taking into account the heterogeneity and complexity of the services and applications, a decentralised approach for the architecture of the TMS is considered in this research. For trust evaluation, two cases are defined in this publication. The first one is evaluating trust of a newly provided service. The second case deals with the trust evaluation of existing services. For a new provided service, trust has to be computed and evaluated by integrating this process into the test framework with the Test Master and Test Agents defined in [2]. Trust computation and evaluation for existing services and applications is made with a completely different approach. For this case, an autonomous decentralised TMS is introduced and trust is evaluated based on the behaviour of each service using trust agents which will be automatically assigned to new entering peers.

There are different trust metric parameters defined in [27-32] which are not completely suitable or enough for our TMS because they are used in different scenarios which do not consider the special application composition nature of the P2P4M2M framework. Furthermore, they are not applicable for evaluating trust of an entering service. This publication defines different trust metric parameters for each of the two cases described above. Reference [33] identifies three perspectives of metrics, such as network performance metrics, knowledge quality metrics and accuracy of detection metrics.

In order to compute the trust level of services and applications in the P2P4M2M framework, we identified a fourth metric perspective, namely, the service availability metric. For a newly provided service, we defined the corresponding metric parameters: Trust based on the functionality of the service - the service description corresponds to the service functionality. DoS attacks - the reaction of the service against a huge number of service requests. This attack gives the opportunity to figure out the robustness of the service and its willingness to accept service requests. Based on its performance against DoS attacks, part of the initial trust level can be derived. For computing trust based on the availability of the services, the following metric parameters for existing services are defined: Number of attendance of a service in various applications. Time a service stays online and time a service stays offline [34]. Number of online/ offline actions. Number of execution times. Number of subscribe-messages and accepted-/ not accepted-messages.

The SMF introduced in [5] and used in the P2P4M2M framework [2] provides no environment for dealing with security and computing trustworthiness of a peer. In order to decentralise the procedure for computing trust and also for using the SMF to make services more secure, a Service Trust Platform (STP) is integrated to the SMF. The Service Trust Platform consists of a trust agent, trust profile, trust metrics and security information. The trust agent has to collect specific trust related data of the communication between services. The trust agent will interact with other trust agents which all together are part of a P2P network using the overlay for storing the shared information about the trustworthiness of a service. Additionally, the trust evaluation and the trust level assessment are made by the trust agent. The security information part will contain relevant security information about the P2P community and different security behaviour policies and preventing information against security attacks. The evaluated and assessed level of trust is permanently updated in the trust profile. Misbehaviour and history information are also included in the profile. Fig. 4 shows an overview about the STP which is included in the SMF of a peer.

V. Application Example

In order to demonstrate the procedure for computing and evaluating trust of services in the P2P4M2M framework two cases are considered for illustration.

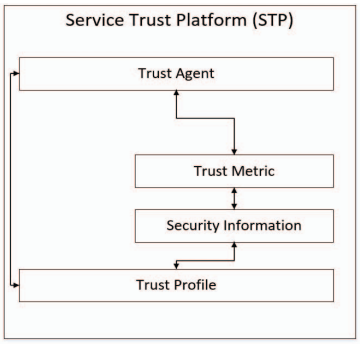

Fig. 4. Overview of STP

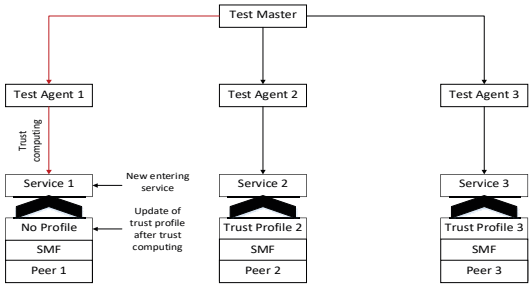

Fig. 5. Computing trust of an entering service using the testing framework

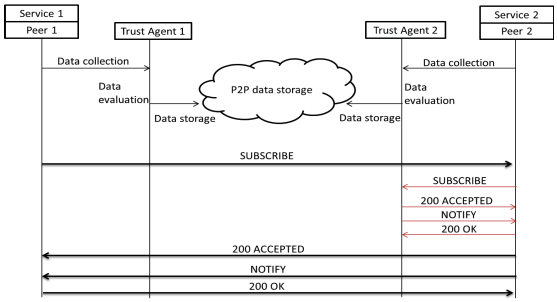

Fig. 6. Example of trust computation for existing services

A. Newly provided service in the M2M community

After service 1 enters the M2M community, its functionality will be tested using the test framework described in [3]. Moreover, using this test architecture presented it is possible to derive the initial trust level and to check whether or not the service entered the community is trustworthy. Based on the functionality of the service, the TGE [3] will generate suitable test cases for security tests and the test agents will execute these cases on the service. After the test is executed, the Test Master will receive the test report and will evaluate the trust level of the entered service 1. Then, the Test Master will send the trust information via the trust agent to the peer who is providing the service. The trust information will be sent to the new introduced STP within the SMF which is included in the peer. The STP will create a profile which include the trust level of a new service. Fig. 5 shows the integration of the TMS inside the testing framework and the above presented workflow of computing trust for an entering service.

B. Interactions between two existing services

Existing services will have an initial trust level based on the initial testing after entering the community described in the above use case. Fig. 6 shows an example of interactions between two services and the trust data collection/ evaluation using trust agents. After that, the trust agent assigned to the peer will measure different trust metric parameters in order to compute trust. The services will communicate with each other using SIP SUBSCRIBE and NOTIFY messages as introduced in [2]. Service 1 is trying to subscribe service 2 by sending a SUBSCRIBE message. During their life time the activities of two services are monitored based on the defined trust metric parameters. These are included at the STP of each peer. After receiving the SUBSCRIBE-message, service 2 will ask trust agent 2 about the trust level of service 1. Trust agents are

connected P2P and evaluated data are stored in the P2P data stores. Trust agent 2 will inform service 2 about the trust level of service 1 and based on that value service 2 will decide to accept or not to accept a session with service 1.

VI. CONCLUSION

Despite the fact that service and application provision in M2M renders many advantages, it also forms an attractive platform for many attackers and malicious peers. This publication presents the so far missing security risks and requirement for the P2P4M2M framework. A novel comparison table of P2P protocols based on the level of security against different attacks is presented. Furthermore, the concept of trust is introduced and major requirements for an effective and stable trust management concept are presented. Based on the special conditions of the P2P4M2M framework, the security requirements and the trust management requirement, a novel trust management system concept considering the initial trust level is presented. This concept enables the trustworthy service and application provisioning in M2M and decreases the risks of security attacks.

ACKNOWLEDGEMENTS

The research project P2P4M2M providing the basis for this publication was partially funded by the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany under grant number 03FH022IX5. The authors of this publication are in charge of its content.

REFERENCES

[1] ETSI TR 102 725, V1.1.1, 2013-06: Technical Report, "Machine-to-Machine communications (M2M); Definitions", ETSI TISPAN

[2] M. Steinheimer, U. Trick, W. Fuhrmann and B. Ghita, "P2P-based community concept for M2M Applications", FGCT 2013, London, UK, December 2013

[3] B. Shala, P. Wacht, U. Trick, A. Lehmann, B. Ghita and S. Shiaeles, "Framework for Automated Functional Testing of P2P-based M2M applications," 9th International Conference on Ubiquitous and Future Networks (ICUFN), in press, 2017

[4] M. Steinheimer, U. Trick, B. Ghita and W. Fuhrmann, "Decentralised System Architecture for autonomous and cooperative M2M Application Service Provision", International Conference on Smart Grid and Smart Cities (ICSGSC), in press, 2017

[5] M. Steinheimer, U. Trick, P. Ruhrig, R. Tönjes, M. Fischer and D. Hölker, „SIP-basierte P2P-Vernetzung in einer Energie-Community", ITG-Fachbericht 242: Mobilkommunikation, pp. 64, Mai 2013

[6] M. Kappes,"Netzwerk- und Datensicherheit", Springer, Wiesbaden, Germany, ISBN: 978-3-8348-0636-9. 2013

[7] J. Vacca, "Computer and Information Security Handbook", Elsevier, Burlington, USA, ISBN: 978-0-12-394397-2. 2013

[8] A. Barki, A. Bouabdallah, S. Gharout and J. Traore, "M2M Security: Challenges and Solutions," IEEE Communications Surveys & Tutorials, Volume: 18, Issue: 2, 2016

[9] European Union Agency for Network and Information Security (ENISA), "Ad-hoc & sensor networking for M2M Communications – Threat Landscape and Good Practice Guide", 2017

[10] European Union Agency for Network and Information Security (ENISA), "Threat Landscape and Good Practice Guide for Smart Home and Converged Media", 2014

[11] X. Nie and X. Zhai, "M2M Security Threat and Security Mechanism Research", 3rd International Conference on Computer Science and Network Technology, 2013

[12] ITU-T, Framework for secure peer-to-peer communications, X.1161, 2008

[13] Z. Trifa and M. Khemakhem, "Taxonomy of Structured P2P Overlay Networks Security Attacks", International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2012

[14] E. Sit and R. Morris, "Security Considerations for Peer-to-Peer Distributed Hash Tables", International Workshop on Peer-to-Peer Systems, Springer, 2002.

[15] E. Keong Lua, J. Crowcroft, M. Pias, R. Sharma and S. Lim, "A Survey and Comparison of Peer-to-Peer Overlay Network Schemes," IEEE Communications Surveys & Tutorials. vol. 7,no. 2, pp. 72.93, 2005

[16] T. Reidemeister, K. Böhm, P. Ward and E. Buchmann, "Malicious Behaviour in Content-Addressable Peer-to-Peer Networks", 3rd Annual Communication Networks and Services Research Conference, 2015

[17] M. Srivatsa and L. Liu, "Vulnerabilities and security threats in structured overlay networks: A quantitative analysis", ACSAC`04, pp.252-261, IEEE, Los Alamitos, 2004

[18] G. Ciaccio, "Recipient Anonymity in a Structured Overlay", AICT-ICIW`06, IEEE, 2006

[19] A. Malatras, "State of the art survey on P2P overlay networks in pervasive computing environments", Journal of Network and Computer Applications, Elsevier, vol. 15, pp. 1-23, 2015

[20] J. Arnedo-Moreno and J. Herrera-Joancomarti, "A survey on security in JXTA applications", Journal of Systems and Software, Elsevier, vol. 82, nr. 9, pp.1513-1525, 2009

[21] G. Dosanjh, B. Lodmell, A. Van Der Star and S. Wang, "Gnutella Peer-to-Peer Security", 2007, available from: https://courses.ece.ubc.ca/cpen442/previous_years/2007_1_spring/modules/term_project/reports/2007/gnutella_security.pdf [23 June 2016]

[22] I. Clarke, O. Sandberg, B. Wiley and T. Hong, "Freenet: A Distributed Anonymous Information Storage and Retrieval System", Proc. ICSI Workshop, Berkeley, CA, June 2000

[23] J. Liang, R. Kumar, K. Ross, "The FastTrack overlay: A measurement study", Computer Netzworks, 50(6):842-858, 2006.

[24] C. Selvaraj and S. Anand, "A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks", Computer Science Review, Elsevier, p. 145-160, 2012

[25] J. Buford, H. Yu, E. K. Lua, " P2P Networking and Applications", Elsevier, Burlington, USA, ISBN: 978-0-12-374214-8. 2009

[26] ITU-T, Technical Report, Trust Provisioning for future ICT infrastructures and services, 2016

[27] F. Boustanifar and Z. Movahedi, "A Trust-Based Offloading for Mobile M2M Communications", Ubiquitous Intelligence & Computing, IEEE, 2016

[28] C. V. L. Mendoza and J. H. Kleinschmidt, "Mitigating On-Off attacks in the Internet of Things using a distributed trust management scheme", International Journal of Distributed Sensor Networks, 11 (11), 2015

[29] R. Chen, J. Guo and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition", IEEE Transactions on Services Computing, Volume: 9, Issue: 3, 2016

[30] D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang, "TRMIoT: a trust management model based on fuzzy reputation for internet of things", Computer Science and Information Systems, vol. 8, no. 4, 2011

[31] Y. B. Saied, A. Olivereau, D. Zeghlache, M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach", Computers & Security, 39, 351-365, 2013

[32] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communieties", IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, 2004

[33] Z. Movahedi, Z. Hosseini, F. Bayan and G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", IEEE Communications Surveys & Tutorials, vol.18, no.2, 2016

[34] ITU-T, "Security requirements and mechanisms of peer-to-peer-based telecommunication networks", X.1163, 2015