

### 3.3. Exemplo de Funcionamento

A operação do GALENA no suporte à autenticação em um ambiente urbano composto de múltiplos domínios de aplicação, como Sistemas de Transporte Inteligente (STI) e Iluminação Pública Inteligente (IPI), é ilustrada. Neste ambiente os dispositivos IoT estão embarcados nas estruturas da cidade e muitos deles são móveis com velocidades de acordo com o perfil do objeto. Os dispositivos também interagem em áreas e regiões distintas da cidade, e em diferentes instantes de tempo. Além disso, eles trocam mensagens para acordar a oferta de serviços entre si, como, por exemplo, informações de tráfego. Lembrando que o GALENA atua nas fases de *Descoberta*, *Socialização* e *Avaliação das Políticas*, e a definição do mecanismo de Autenticação, sendo a autenticação feita externamente. A Figura 1 ilustra uma interação entre dispositivos de STI (semáforo inteligente e ônibus inteligente) e de IPI (poste de iluminação inteligente) e um dispositivo pessoal (smartphone). Os sinais sem fio (*wireless*) representam os dispositivos dentro do mesmo raio de transmissão e capazes de trocar mensagens e descobrir os serviços disponíveis. Neste caso, na figura um conjunto de dispositivos  $d_1, d_2, d_3, d_4$  possuem identificadores únicos, rotulados respectivamente como A, B, C e D; e suportam os mecanismos de autenticação  $m_1, m_2$  e  $m_3$  correspondentes a RSA, ECC e PUF, respectivamente.

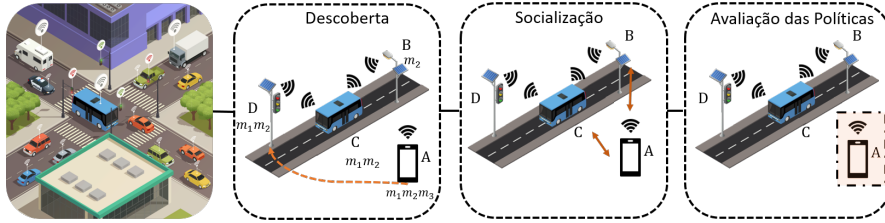


Figura 1. Operação do GALENA em um ambiente IoT de STI e IPI

Na fase de Descoberta, os quatro dispositivos IoT estão próximos e tornam-se ciente uns dos outros. O dispositivo  $A$  então autonomamente solicita a  $D$  um serviço  $s_1$ , referente a informações de tráfego. Entretanto, na fase de Socialização,  $A$  por nunca ter interagido com  $D$  não possui um valor de confiança social direta a respeito dele. Assim, para derivar um valor de confiança social, ele inquirir os outros dispositivos próximos ( $B$  e  $C$ ) sobre a confiança social que eles possuem a respeito de  $D$ , obtendo como respostas os valores 0,7 e 0,8, respectivamente. A partir desses valores,  $A$  então determina o valor das recomendações  $R = 0,75$ . Ainda, considere que  $A$  e  $D$  não ofereçam o mesmo conjunto de serviços, logo seus  $WOR$  é igual a 0, e estão próximos entre si com  $LOR$  de 0,95. Ademais,  $A$  tem os seguintes parâmetros configurados para a Equação 1,  $\alpha = 0,5$ ,  $\beta = 0$ ,  $\gamma = 0,5$ , e na Equação 2,  $\delta = 0,5$ ,  $\mu/\pi = 0$ . Assim,  $\mathcal{ST} = 0,5 * 0,95 + 0,5 * (0 + (1 - 0,5) * 0,75) = 0,66$ . A fase de Avaliação das Políticas ocorre após a fase de Socialização. Nesta fase, o dispositivo verifica quais são as políticas associadas aquele ambiente. Neste caso, para o ambiente “rua”, o dispositivo  $A$  possui a seguinte política configurada pelo usuário:  $\mathcal{P}_1 = \langle \mathcal{F}(*), \{m_1, m_2\}, \mathcal{ST}_{Id} > 0,65, \mathcal{C}(\text{“rua”}) \rangle = P_2^{ECC}$ . Desta forma,  $A$  emprega o perfil  $P_2^{ECC}$  como mecanismo de segurança para a autenticação, visto que as características do dispositivo  $D$  correspondem às determinadas pela política. Esse processo ocorre paralelamente em  $D$ . Por fim, os dois dispositivos se autenticam usando o mecanismo selecionado ( $P_2^{ECC}$ ) e  $D$  provê o serviço de informação de tráfego solicitado ( $s_1$ ). Assim, o GALENA permite os dispositivos do STI, IPI e pessoais (smartphones) definam

autonomamente um perfil de autenticação adequado ao ambiente e à relação social.